



Council of the European Union  
General Secretariat

Brussels, 15 October 2021

---

---

**Interinstitutional files:  
2020/0361(COD)**

---

---

**WK 12332/2021 INIT**

**LIMITE**

**COMPET  
MI  
JAI  
TELECOM  
CT**

**PI  
AUDIO  
CONSUM  
CODEC  
IA  
JUSTCIV**

**WORKING PAPER**

*This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.*

**NOTE**

---

From:	NL delegation
To:	Working Party on Competitiveness and Growth (Internal Market)
Subject:	Digital Services Act (DSA) Addressing the issue of abuse of hosting for manifestly criminal offences

---

---

WK 12332/2021 INIT

**LIMITE**

**EN**

**Digital Services Act (DSA)**  
**Addressing the issue of abuse of hosting for manifestly criminal offences**

**Problem definition: The abuse of hosting services for criminal activity**

Criminal activity online is an escalating challenge. This growth was already apparent before the COVID pandemic spurred business and civil activities to migrate online, and the growth has accelerated ever since. The services of hosting providers are being abused for many types of serious crime. Many types of serious crime perpetrated online, such as the dissemination of malware (including ransomware) and Child Sexual Abuse Material (CSAM), types of fraud and the trading of illegal goods such as weapons and drugs, need hosting services to achieve the scale we see today.

Many hosting providers take measures against the abuse of their services for such illegal activities. Unfortunately, there are also hosting providers who do not take sufficient, or even basic measures. This gives criminals the opportunities they need for their actions, resulting in more crime and more victims online, and greater challenges for law enforcement. An obligation to take adequate measures would help mitigate the risk of abuse and reduce serious crime and the number of victims on the internet, while creating a level playing field for those hosting providers that already act responsibly.

After having circulated our original amendment in the Internal Market Working Party and other relevant Council configurations, it became apparent that whilst some could support our text, there was no majority for our suggestions. To this end, we have drafted an alternative text which we believe could be more amenable to a majority of the Member States. To support a fruitful and open discussion, we have set out an alternative below which provides for concrete, specific obligations, commensurate with the concrete nature of clear-cut due diligence obligations incumbent on online intermediaries that fall within the scope of the DSA. This may limit the flexibility of the regulation, but would provide for more legal certainty for hosting providers. For delegations' ease of reference and to compare the original proposal with the alternative, we have placed the original proposal in the Annex of this note (please refer to page 3 of this document).

The original proposal also raised the question as to whether the measures should apply to all hosting providers, or only hosting providers that are not online platforms. Finally, we aim to exclusively target users that "pay" for the use of hosting services by pecuniary means, whichever form and/or shape this may take, e.g. regular or virtual currencies. We do not intend to capture those users who use "free" services, e.g. registering for a Gmail account for private correspondence use. However, given that we are unsure about which term may be most appropriate in EU law to delineate such users, we would like to call on, and be greatly appreciative of, the European Commission's and Council legal services' help in this regard.

We hope to have an open discussion on this issue, including on the question whether to limit the scope to providers of hosting services that are not online platforms, or to apply our suggestions to online platforms also.

**Text proposal Chapter III, section 2**

Article 15b alternative

Measures and protection against misuse

Providers of hosting services [that are not online platforms] shall

1. ensure that paying users can only use its services when the provider has obtained the name, address, telephone number, electronic mail address and bank account details of the user. Art. 22.2 – 22.5 are applicable;
2. connect to available information sources to obtain, or be able to receive, and adequately process information on manifestly criminal offences and vulnerabilities regarding their networks and the type of service they provide;
3. take immediate measures to prevent further harm when knowledge is obtained about manifestly criminal offences being committed through the use of its services and the continuation of those manifestly criminal offences may result in serious harm;
4. promptly inform recipients of the services when knowledge is obtained about manifestly criminal offences being committed through or by those recipients, or when knowledge is

obtained about serious vulnerabilities in hardware or software that can be abused for such offences;

5.
  - (a) suspend, for a reasonable period of time and after having issued a prior warning, the provision of their services to recipients of the service that frequently provide manifestly criminal content or commit manifestly criminal offences;
  - (b) assess, on a case-by-case basis and in a timely, diligent and objective manner, whether a recipient, individual or entity engages in the misuse referred to in paragraph 5, sub (a), taking into account all relevant facts and circumstances apparent from the information available to the provider. Those circumstances shall include at least the following:
    - i. the absolute numbers of items of manifestly criminal content or manifestly criminal offences, submitted in the past year;
    - ii. the relative proportion thereof in relation to the total number of items of information provided in the past year;
    - iii. the gravity of the misuses and its consequences;
    - iv. the intention of the recipient, individual or entity.
  - (c) set out, in a clear and detailed manner, their policy in respect of the in their terms and conditions, including as regards the facts and circumstances that they take into account when assessing whether certain behaviour constitutes misuse, and the duration of the suspension.

Accompanying Recital (XX):

Article [15b] requires providers of hosting services [that are not online platforms] to take basic measures in order to address the risk of misuse of their services for manifestly criminal offences and to mitigate it if any actual misuse occurs. Examples of manifestly criminal activities are the dissemination of CSAM, malware (including ransomware) and phishing emails, and the hosting of malicious or fraudulent webshops. Public and private information resources are often available to inform hosting providers of known software vulnerabilities, threats, abuse and cybercrime incidents. Examples are Computer Emergency Response Teams (CERTs) and available abuse feeds. Providers of hosting services should connect to these information sources to obtain this information. In some countries, such information can also be shared with providers of hosting services without prior request. Providers of hosting services should have procedures and technical measures in place which enables them to process this information adequately, and act accordingly if needed. These measures should be carried out in a reasonable, proportionate, effective and non-discriminatory way.

## ANNEX

Criminal activity online is an escalating challenge. This growth was already apparent before the COVID pandemic spurred business and civil activities to migrate online, and the growth has accelerated ever since. Many types of serious crime perpetrated online, such as the dissemination of malware (including ransomware) and Child Sexual Abuse Material (CSAM), types of fraud and the trading of illegal goods such as weapons and drugs, need hosting services to achieve the scale we see today. The services of hosting providers are therefore being abused for many types of serious crime.

Many hosting providers take measures against the abuse of their services for such illegal activities. Unfortunately, there are also hosting providers who do not take sufficient, or even basic measures. This gives criminals the opportunities they need to conduct their actions, resulting in more crime and more victims online, and greater challenges for law enforcement. An obligation to take adequate measures, depending on the specific business, services and risks, would help mitigate the risk of abuse and reduce serious crime and the number of victims on the internet, while creating a level playing field for those hosting providers that already act responsibly.

For online platforms, the exemption of liability puts a premium on not having actual knowledge of illegal content. Notice-and-take-action mechanisms to counter this have proved insufficient. The current DSA proposal does not provide for possibilities to hold online platforms to account for making public and disseminating illegal content. Many online platforms, especially those that are very large, already have systems in place to counter illegal content. However, manifestly criminal offences is, after being noticed on very large platforms, often moved to alternative, smaller platforms that have less sophisticated means to counter it, moving the risk from large to smaller platforms.

The proposal below aims to address these risks. It has a similar setup as Articles 26 and 27 of the current DSA proposal: it requires hosting providers to assess risks and take measures accordingly. Its applicability does not depend on the size of the hosting provider. Small hosting providers are not less vulnerable to abuse than larger ones. Therefore, measures to be taken should depend primarily on assessed risks.

Importantly, general content monitoring should not be required and hosting providers should fully respect fundamental rights, in particular the right to freedom of speech. The specific type of measure could be left to the hosting provider. Ideally, measures chosen are regarded as (existing) best practices in the hosting sector. Because of the dynamic nature of the market, what is considered as best available measures may change over time. Therefore, the proposal allows for flexibility for developments in the sector, making it future proof.

The proposal should not be understood as necessarily and immediately leading to a much higher degree of content moderation throughout. Instead, it should be understood as a way to force certain hosting service providers to catch up. It is primarily targeted at mala fide hosting service providers and providers that are lagging behind significantly. It prevents content providers from migrating to another hosting service provider in order to more easily disseminate illegal content.

To ensure compliance by all hosting providers that provide services in the Union, Articles 41 and 42 DSA would give the Digital Service Coordinator the power to enforce these obligations, including the power to impose proportionate remedies where the measures of the service provider are deemed insufficient. Finally, to avoid fragmentation of the internal market and ensure uniform application of these obligations, the European Commission, in conjunction with the Board (OR: and/or) could be empowered to issue interpretative guidelines

### **Text proposal Chapter III, section 2**

#### **Art. 15b**

1. Services providers shall identify, analyse and assess at least once a year any significant risk for the misuse of their services for manifestly criminal offences stemming from the functioning and use made of their services in the Union.
2. Without prejudice to article 7 providers of services shall put in place reasonable, proportionate, effective and non-discriminatory mitigation measures to address the risk and, if any, actual misuse of their services for manifestly criminal offences.

3. The decision as to the choice of these measures shall remain with the service provider with due regard to their size and level of risk of misuse for manifestly criminal offences. Such measures may include:

a) an acceptable use policy regarding what is expected of the recipients of the services in case of manifestly criminal offences, and to suspend the services to, and/or end the contractual relationship with the recipient of the services who regularly or consistently does not act upon manifestly criminal offences

b) immediate measures to prevent further harm when knowledge of manifestly criminal offences is obtained and the continuation of those manifestly criminal offences may result in serious harm. Examples of such offences are the dissemination of CSAM, malware (including ransomware) and phishing emails, and the hosting of malicious or fraudulent webshops.

c) to ensure correct and up to date customer details, for (but not only) direct contact in case of manifestly criminal offences

d) proactive engagement with recipients of services in case of manifestly criminal offences or vulnerabilities in hardware or software that can be abused for such offences

e) industry best practices to prevent and address manifestly criminal offences

f) adequate measures that can reasonably be expected to obtain information on vulnerabilities or manifestly criminal offences regarding their networks and services, for example by connecting to available information sources

g) adequate measures that can reasonably be expected to diminish the effects of manifestly criminal offences on their networks for other users in general