Technology Ireland's response to Coimisiún na Meán's e-CommerceT Compliance Strategy Consultation

Introduction

Technology Ireland, the Ibec group representing the technology industry, welcomes the opportunity to respond to Coimisiún na Meán's ("**CnaM**") e-Commerce Compliance Strategy (the "Strategy") Consultation relating to Online Safety Codes, Online Safety Guidance Materials and Advisory Notices.

Since March 2019, when the Government first announced its intention to bring forward online safety legislation, as seen in the development of the Online Safety and Media Regulation ("**OSMR**") Act transposing the revised Audiovisual Media Services Directive ("**AVMSD"**) into Irish law, Technology Ireland has been consistent in supporting its goals to promote online safety through a systemic approach to oversight of online platforms and digital services.

We very much welcome and support all efforts of CnaM to engage with stakeholders with a view to ensuring that all proposals concerning the OSMR are effective, practical, proportionate, and legally robust in line with the objectives to be achieved and harmonised with existing laws and regulations.

We recognise the Strategy as an extremely important safeguard for ensuring that the Online Safety Codes (the "**Codes**") and any guidance developed under the framework of the OSMR do not conflict with Union law.

We note that this important aim has been reflected throughout the legislative process of the OSMR: for example, the General Scheme of the OSMR Bill expressly provided that the Codes will include:

> *"Extensive consideration of Union law, particularly related to the revised Directive and the legal liability regime for online services provided for by the eCommerce Directive (Directive (EC) 2000/31)"*[1]

This aim is now even more important given the significant risk of overlaps/conflicts arising between this framework and Regulation (EU) 2022/2065 on a Single Market for Digital Services (the "**DSA**").

Submission

Technology Ireland has reviewed the 13 points raised in the Draft e-Commerce Compliance Strategy and our response to this consultation is outlined below.

At the outset, we wish to recognise that many aspects of the proposed approach outlined in the Consultation document take a sensible approach to ensuring the purpose of the Strategy is achieved. The purpose of the Strategy, as expressly stated in the OSMR, is to ensure that the OSMR Codes and guidance do not contain any obligations which are inconsistent with the safe harbour protections set down under Directive 2000/31/EC ("**eCD"**) which are now restated and/or amended under Articles 4-8 of the DSA (the "**Safe Harbour Protections**").

In particular, the safeguards outlined in points (2), (3) and (6) of Appendix 2 of the Consultation are important measures that go towards reflecting this purpose.

[1] General Scheme of the Online Safety and Media Regulation Bill, published on 8 December 2020

General Points

We have the following overarching concerns with the proposed approach taken in the Consultation:

i. **Certain aspects of the proposed approach cut across the harmonisation objectives of the DSA**

The DSA prohibits Member States from adopting additional national laws on the matters covered by the DSA, given that "diverging national laws negatively affect the internal market" (see Recital 2 DSA); and emphasises the importance of the uniform application of the DSA's harmonised rules, so as to "put an end to fragmentation of the internal market" and "ensure legal certainty" (see Recital 4 DSA).

Recital 9 of the DSA expressly recognises requirements addressing the dissemination of illegal content online as an area which should be fully harmonised under the DSA and, accordingly, requires Member States not to adopt national measures dealing with this area.

However, in a number of respects the proposed approach outlined in Appendix 2 of the Consultation envisages that the Strategy will allow CnaM to include provisions in the Codes that cut across areas reserved for the DSA:

- point (5) of Appendix 2 expressly envisages that the Codes, on a general basis, may require providers to take measures to reduce the risk of dissemination of unlawful content, whereas this is a field exclusively regulated by the DSA scheme. Specifically, the DSA requires providers of very large online platforms (VLOPs) and very large online search engines (VLOSEs) to identify, analyse and assess systemic risks in the EU stemming from the design, functioning or use made of their services, including the risk of dissemination of illegal content through their services. The DSA only introduces such a risk assessment regime for VLOPs and VLOSEs and not for other providers of intermediary services. Given the harmonised, deliberately, and carefully graduated approach of the DSA, Member States may not impose "VLOP/VLOSE-like" obligations on providers of intermediary services that do not qualify as such under the DSA.

- point (4) of Appendix 2 also provides that the Codes may redefine the liability exemption expressly set out under Art 6 of DSA (see further below).

In this regard, we would note that the General Scheme of the OSMR Bill, as submitted[2] to the European Commission through the technical regulation information system (TRIS) notification process[3] on 10 December 2020, specifically provided for the fact that the Codes would include extensive consideration of Union law, to ensure harmonisation.

In our view, failure to provide for this in the Strategy (as well as the broader framework of OSMR more generally) would require serious consideration as to whether the Strategy would need to be submitted through the TRIS notification process to consider whether it ensures appropriate harmonisation with EU legislation as envisaged in the General Scheme that was previously notified.

[2] https://technical-regulation-information-system.ec.europa.eu/en/notification/23358

[3] The TRIS process requires that any technical regulation on information societies services must be notified to the European Commission to ensure that national legislation does not conflict with EU legislation

Proposed Solution: The Strategy should include a provision requiring that all Codes contain a provision to the effect that where a requirement contradicts or overlaps with a DSA requirement, a provider shall not be guilty of contravention where it has complied with the requirements of the DSA. Point (11) of Appendix 2 should be modified to state that CnaM will invite views on whether the proposed Codes contain provisions that are inconsistent with any provision of the DSA. Point (5) of Appendix 2 should be removed to ensure consistency with the DSA, including Articles 34-35 DSA.

ii. **Overall, the proposed approach fails to recognise certain aspects of the Safe Harbour Protections**

As above, the purpose of the Strategy, as expressly stated in the OSMR, is to ensure that OSMR Codes and guidance are consistent with the Safe Harbour Protections. However, we have concerns that the approach outlined in the Consultation would not sufficiently ensure consistency with these provisions in all material respects. In particular, we note the following:

- The Consultation document fails to recognise the "Good Samaritan" clause introduced by Article 7 DSA. Article 7 DSA extends the safe harbour liability regime by providing for a new Safe Harbour Protection that allows an intermediary service provider to carry out voluntary own initiative investigations or similar measures against illegal content, while retaining the benefit of the liability exemptions. This is an important protection that needs to be reflected in the Strategy.

- Point (3) of Appendix 2 appears to limit the Safe Harbour Protections to hosting services only as it seeks to apply the "actual knowledge" test applicable to hosting providers under Article 6 DSA to all providers of designated services under OSMR. Providers of designated services under OSMR are not limited to hosting services and, as expressly envisaged under s139L OSMR, may also include mere conduit services (as per Article 4 DSA) and caching services (as per Article 5 DSA).

- Lastly the Consultation document also suggests that the Strategy would only have to ensure that the Codes (and not online safety guidance materials and advisory notices) comply with the liability exemptions. This is on the basis that a failure to comply with online safety guidance materials and advisory notices would not give rise to a contravention under OSMR. This is contrary to the express wording of S139ZF OSMR which requires that the Strategy should ensure compliance by all elements of the Relevant Provisions with the Safe Harbour Protections. These guidance materials and advisory notices may well become the standard to which providers may be held to account and, as such, should also reflect the safe harbour regime in full.

Proposed Solution: (i) points (2) and (3) of Appendix 2 should be expanded to also make specific reference to guidance materials and advisory notices, (ii) point (2) of Appendix 2 should be expanded to make specific reference to Art 7 of the DSA and (iii) additional language should be included in point (3) of Appendix 2 to provide for caching and mere conduit services.

B. Approach to consistency with exemptions from liability

Technology Ireland believes that the proposed approach under Section B fails to sufficiently ensure consistency with Articles 4, 5 & 6 of the DSA.

Section 139ZF OSMR expressly provides that the purpose of the Strategy is to set out CnaM's approach to ensuring that the Codes, online safety guidance materials and advisory notices (together the "**Relevant Provisions**") do not contain any obligations which are inconsistent with the Safe Harbour Protections. More particularly, Articles 4, 5 & 6 of the DSA outline important liability exemptions that apply to information society service providers ("**ISP**").

> **2. Online safety codes will therefore not contain any provision which makes it a contravention for a designated service provider to transmit or host unlawful content, as long as the provider complies with the conditions in Regulations 16 to 18 of the 2003 Regulations (or the corresponding conditions in Article 4, 5 and 6 of the Digital Services Act).**
>
> **3. In order to remove any doubt, each online safety code will contain a provision to the effect that, notwithstanding any other provision of the online safety code, a designated service provider shall not be guilty of a contravention by reason only of the presence on its service of unlawful content when it had no actual knowledge of the unlawful nature of the content.**

While points (2) and (3) of Appendix 2 provide for an overriding requirement that the Codes would ensure compliance with these protections, we have a number of concerns that the approach outlined in the Consultation fails to ensure that these liability exemptions will be appropriately reflected in measures outlined in the Relevant Provisions.

Point (3) seems to imply that a service provider could be guilty of a contravention once it acquires actual knowledge of the unlawful nature of the content. However, the safe harbours are available as long as it 'acts expeditiously' upon obtaining knowledge. This should be made clearer.

> **4. However, online safety codes may contain provisions that make it a contravention not to remove unlawful content expeditiously once the provider becomes aware of the unlawful nature of the content and may further specify what would be regarded as expeditious in particular cases.**

Whereas Article 6 of the DSA expressly provides for a liability exception where a provider acts expeditiously to remove/disable content on becoming aware of its illegality, point (4) envisages that the Codes may prescribe what may constitute "expeditious" for these purposes. Prescribing how "expeditious" should be understood in this context would likely narrow the limitation of liability provided for in Article 6 of the DSA and, as a result, significantly limit the application of this important safeguard. The DSA pre-empts the ability of Member States to lay down specific turn-around times for the removal of allegedly illegal content. This suggested approach also fails to recognise the need for a balancing assessment regarding the rights of affected individuals with respect to each removal or disable as specifically required under the DSA and would, again, be a departure from the harmonised approach required under the DSA[4].

[4] Recital 22 of the DSA

5. Online safety codes may contain provisions that require providers to take measures that reduce the risk of unlawful content on their services. Failure to implement those measures may amount to a contravention.

Point (5) appears to be suggesting that notwithstanding the overriding requirements set out in point (3), the Codes may "*contain provisions that require providers to take measures that reduce the risk of unlawful content on their services*". If this is intended as a permitted exemption to the overriding requirement to ensure compliance with the liability exemptions, this raises very significant concerns as this undermines the purpose of the Strategy – which is to ensure consistency with the Safe Harbour Protections. Further, the vague language included in point (5) could allow broad scope for departure from the Safe Harbour Protections and, as such, there would be significant risk of conflict with EU law.

If an online safety code provides for such a contravention, it should specify the factors that constitute awareness having regard to Recital 53 of the DSA and the case law of the Court of Justice of the European Union (CJEU).

Proposed Solution: Point (5) should be removed to ensure consistency with the DSA, including Articles 34-35 of the DSA. The Strategy should clarify that any measures included in the Relevant Provisions would be subject to the safeguards set out in points (2), and (3) without exemption. Points (4) and (5) should at a minimum be expressed as being subject to points (2) and (3) above. The application of the safeguards provided for under points (2) and (3) should also extend to online safety guidance materials and advisory notices. Point (3) should make it clear that the safe harbours are available as long as the provider 'acts expeditiously' upon obtaining knowledge, to ensure consistency with the DSA.

C. Approach to consistency with Article 15 of the e-Commerce Directive / Article 8 of the Digital Services Act.

At the outset, it is important to note that our members regard the prohibition under Article 8 of the DSA as vitally important. It is central to the proper functioning of the intermediary liability regime and to the appropriate safeguarding of freedom of expression and other fundamental rights. Moreover, if general monitoring obligations could be imposed on service providers, it would defeat or seriously undermine the safe harbours conferred by Articles 12-14 of the e-Commerce Directive (or Articles 4-7 of the DSA), including for hosting services whose safe harbour is conditional on not having actual knowledge or awareness of illegal activity.

There are, however, provisions relating to proactive monitoring that could bear some clarification. In particular, while the e-Commerce Directive provided, and the CJEU consistently held, that an intermediary cannot be compelled to undertake an obligation to actively monitor all the data of all its customers, Recital 30 of the DSA states that "monitoring obligations in a specific case" may be allowed.

In practice, depending on the way in which an order is framed, monitoring obligations in a specific case can have the practical effect of requiring the general monitoring of all the intermediary's data of all its customers, which would clearly run afoul of the prohibition on a general obligation to monitor in Article 15 of the e-Commerce Directive (now reflected in Article 8 of the DSA). An example of this result can be seen in *Glawischnig-Piesczek (discussed further below)*, where the CJEU decision held that a court from a Member State is not precluded by Article 15 of the e-commerce Directive from ordering the removal of identical or "equivalent" content to that which had been declared illegal, and

seeking to limit "equivalent content" to that which is "essentially unchanged", such that the online platform may rely on automation and need not carry out a separate assessment of unlawfulness. In light of the CJEU's significant body of case law dictating the narrow circumstances where monitoring obligations in a specific case may be permitted, and the fact-specific nature of such cases, these types of limited monitoring obligations may be more appropriately addressed (and formulated) by way of fact-specific court injunction measures, rather than being sought to be implemented in systemic obligations contained in the Codes.

However, the Consultation document appears to be attempting to call out a number of exemptions to Article 8 as may be provided for in the OSMR Relevant Provisions. As such, we are concerned that the approach under Section C fails to ensure sufficient consistency with the prohibition on general monitoring (Article 8 DSA).

6. CnaM will not include any provision in an online safety code, online safety guidance materials or an advisory notice ("Relevant Provision") that necessitates general monitoring of content or generally taking active steps to seek facts or circumstances indicating illegal activity.

Whilst this reflects the language of section 139ZF OSMR Act, online safety guidance materials and advisory notices are not in fact binding, so it is unclear why they are discussed here as potentially necessitating general monitoring, etc. This comment also applies to the following paragraphs and so we do not discuss guidance materials and advisory notices further below. However, notwithstanding this assessment and in accordance with General Point (ii) above, online safety guidance materials and advisory notices must remain consistent with the Safe Harbour Protections. As outlined above, s139ZF OSMR requires that the Strategy should ensure compliance by all elements of the Relevant Provisions with the Safe Harbour Protections.

7. CnaM may adopt a Relevant Provision which can be complied with either by general monitoring or in other ways.

The statement above is confusing as it suggests that an online safety code could impose an obligation to such an extent that it would require a general level of monitoring, despite the prohibitions in the e-Commerce Directive and the DSA.

Also, the wording suggests that CnaM may adopt a Relevant Provision which can be complied with either by general monitoring or in "*other ways*". It follows that, if a provider cannot satisfy these requirements in "*other ways*", which for example, may be infeasible or unduly burdensome, the provider must then do so by general monitoring.

Therefore, it should be made clear that when an obligation can be complied with either by general monitoring or in other ways, the "other ways" available must be valid and feasible alternatives so as not to incentivise (effectively require) general monitoring or 'over-removal' by platforms.

8. CnaM may adopt a Relevant Provision that necessitates limited monitoring that does not amount to a general monitoring obligation.

Our members would welcome clarity on the exact legal basis for the inclusion of such an obligation in an online safety code as well as clarity on the relationship between such an obligation and the statutory framework for content limitation notices provided for in Chapter 7 of the OSMR Act (which,

per section 139ZZD(5), also interacts with the Article 15 prohibitions). In particular, if/where they overlap in scope and why one approach would be chosen over another.

It is not clear how an online safety code, which takes a systemic approach to regulation, could conceivably impose a monitoring obligation "*in a specific case*" within the meaning of Recital 30 of the DSA (or of the previously applicable Recital 47 of the e-Commerce Directive as interpreted by the CJEU). For example, in *Glawischnig-Piesczek* (Case C-18/18), the CJEU notes at paragraph 35:

> "*Such a specific case may, in particular, be found, as in the main proceedings, in a particular piece of information stored by the host provider concerned at the request of a certain user of its social network, the content of which was examined and assessed by a court having jurisdiction in the Member State, which, following its assessment, declared it to be illegal*". (Emphasis added).

As is also clear from that case and subsequent CJEU case law, any obligation "*must not, in any event, be such as to require the host provider concerned to carry out an independent assessment of that content*". Indeed, as Advocate General Øe more recently noted in Case C401/19: "*It follows, in general, that, although intermediary providers are technically well placed to combat the presence of certain illegal information disseminated through their services, they cannot be expected to make 'independent assessments' of the lawfulness of the information in question. Those intermediary providers do not generally have the necessary expertise and, above all, the necessary independence to do so – particularly when they face the threat of heavy liability. They cannot therefore be turned into judges of online legality, who are responsible for coming to decisions on legally complex questions*".

It is unclear how CnaM would propose to limit a monitoring obligation to a "specific case" by means of systemic obligations contained in Codes. Even if it were possible to devise case types, this would require an independent assessment from host providers in each individual case as they would need to decide whether an account/content is indeed illegal. Thus, it appears that there is a real risk that an obligation of this nature would not comply with Article 8 DSA (as interpreted by the CJEU).

It is also unclear how the proportionality of the territorial scope of such an obligation would be ensured. For example, the DSA notes that orders 'should not exceed what is strictly necessary' and 'should in principle be limited to the territory of the issuing Member State' (Recital 36). Yet, any online safety code applying to video sharing platform services will, by default, have EU-wide effect.

In light of the above, our members would welcome clarity around how CnaM proposes or intends to apply an obligation of this nature.

In our view, it will be extremely important that the Strategy expressly recognises the general monitoring prohibition and carefully assesses against Article 8 of the DSA and applicable guidance and case law of the CJEU when a specific monitoring obligation may be appropriate, to ensure a proportionate, and legally robust framework and to meet the express requirements of the Strategy as expressly stated in OSMR (this comment is relevant to all obligations herein and not just to general monitoring).

> **9. CnaM may adopt a Relevant Provision that specifies particular circumstances in which designated service providers must take active steps to seek facts or circumstances indicating illegal activity.**

Please see our comments under points 6 and 8 above.

It will be extremely important that the Strategy expressly recognises the general monitoring prohibition and carefully assesses against Article 8 of the DSA and applicable guidance and case law of the CJEU.

Proposed Solution - Part C: If points (7), (8) and (9) are to be included, the Strategy should expressly require that any provisions introduced pursuant to points (7), (8) and (9) must be assessed against applicable CJEU case law and to ensure they comply with Article 8 of the DSA.

11. When consulting on a draft of an online safety code, online safety materials or advisory notices, CnaM will invite respondents' views on whether they contain provisions that are inconsistent with liability exemptions in Regulations 16 to 18 of the 2003 Regulations (or Articles 4, 5 or 6 of the Digital Services Act) or inconsistent with Article 15 of the E-Commerce Directive (or Article 8 of the Digital Services Act).

As per the above:

Proposed Solution: Point (11) of Appendix 2 should be modified to state that CnaM will invite views on whether the proposed Codes contain provisions that are inconsistent with any provision of the DSA.

12. Respondents will be invited to clearly demonstrate how, in their opinion, a provision imposes any such obligation on them. CnaM will consider all responses received in respect of the question and may, if it considers appropriate, update the Relevant Provision of the draft online safety code and guidance material accordingly, to account for the respondents' views.

Notwithstanding our comment under point 6 above, the above sentence seems to omit reference to advisory notices in error.