

Your response

Questions for industry	Your response
<p>Question 1: Are you providing a UK-established service that is likely to meet the AVMSD definition of a VSP?</p> <p>Please provide details of the service where relevant. The establishment criteria under the AVMSD are set out in annex 5.</p>	<p>Confidential? – No</p> <p>No</p>
<p>Question 2: Is your service able to identify users based in specific countries and do you provide customised User Interfaces (UI), User Experience (UX) functionality or interaction based on perceived age and location of users?</p>	<p>Confidential? – No</p> <p>n/a</p>
<p>Question 3: How does your service develop and enforce policies for what is and is not acceptable on your service? (including through Ts&Cs, community standards, and acceptable use policies)</p> <p>In particular, please provide information explaining:</p> <ul style="list-style-type: none"> • what these policies are and whether they cover the categories of harm listed in the AVMSD (protection of minors, incitement to hatred and violence, and content constituting a criminal offence – specifically Child Sexual Exploitation and Abuse, terrorist material, racism and xenophobia); • how your service assesses the risk of harm to its users; • how users of the service are made aware of Ts&Cs and acceptable use policies; and • how you test user awareness and engagement with Ts&Cs. 	<p>Confidential? – No</p> <p>n/a</p>
<p>Question 4: How are your Ts&Cs (or community standards/ acceptable use policies) implemented?</p>	<p>Confidential? – No</p> <p>n/a</p>

<p>In particular, please provide information explaining:</p> <ul style="list-style-type: none"> • what systems are in place to identify harmful content or content that may breach your standards and whether these operate on a proactive (e.g. active monitoring of content) or reactive (e.g. in response to reports or flags) basis; • the role of human and automated processes and content moderation systems; and • how you assess the effectiveness and impact of these mechanisms/processes. 	
<p>Question 5: Does your service have advertising rules?</p> <p>In particular, please provide information about any advertising rules your platform has, whether they cover the areas in the AVMS Directive, and how these are enforced. See Annex 5 for a copy of the AVMSD provisions.</p>	<p>Confidential? – No</p> <p>n/a</p>
<p>Question 6: How far is advertising that appears on your service under your direct control, i.e. marketed, sold or arranged by the platform?</p> <p>Please provide details of how advertising is marketed, sold and arranged to illustrate your answer.</p>	<p>Confidential? – No</p> <p>n/a</p>
<p>Question 7: What mechanisms do you have in place to establish whether videos uploaded by users contain advertising, and how are these mechanisms designed, enforced, and assessed for effectiveness?</p>	<p>Confidential? – No</p> <p>n/a</p>
<p>Question 8: Does your service have any reporting or flagging mechanisms in place (human or automated)?</p> <p>In particular, please provide information explaining:</p>	<p>Confidential? – No</p> <p>n/a</p>

<ul style="list-style-type: none"> • what the mechanisms entail and how they are designed; • how users are made aware of reporting and flagging mechanisms; • how you test user awareness and engagement with these mechanisms; • how these mechanisms lead to further action, and what are the set of actions taken based on the reported harm; • how services check that any action taken is proportionate and takes into account Article 10 of the European Convention of Human Rights (freedom of expression); • how users (and content creators) are informed as to whether any action has been taken as a result of material they or others have reported or flagged; • whether there is any mechanism for users (including uploaders) to dispute the outcome of any decision regarding content that has been reported or flagged; and • any relevant statistics in relation to internal or external KPIs or targets for response. 	
<p>Question 9: Does your service allow users to rate different types of content on your platform?</p> <p>Please provide details of any rating system and what happens as a result of viewer ratings.</p>	<p>Confidential? – No</p> <p>n/a</p>
<p>Question 10: Does your service use any age assurance or age verification tools or related technologies to verify the age of users?</p> <p>In particular, please provide information explaining:</p> <ul style="list-style-type: none"> • how your age assurance policies have been developed and what age group(s) they are intended to protect; • how these are implemented and enforced; • how these are assessed for effectiveness or impact; and • if the service is tailored to meet age-appropriate needs (for example, by 	<p>Confidential? – No</p> <p>ACCS checks that age verification works. We provide audit, certification and an Assurance Scheme for age verification and age assurance.</p>

<p>restricting specific content to specific users), how this works.</p>	
<p>Question 11: Does your service have any parental control mechanisms in place?</p> <p>In particular, please provide information explaining:</p> <ul style="list-style-type: none"> • how these tools have been developed; • what restrictions they allow; • how widely they are used; and • how users of the service, and parents/guardians if not users themselves, are made aware of and encouraged to use the parental control mechanisms that are available. 	
<p>Question 12: Does your service have a complaints mechanism in place? Please describe this, including how users of your service can access it and what types of complaint they can make.</p> <p>In particular, please provide information explaining:</p> <ul style="list-style-type: none"> • any time limits for dealing with complaints; • how complainants are informed about the outcomes of complaints; • any appeals processes, how they work, and whether they are independent from the complaints processes; and • the proportion of complaints which get disputed or appealed. 	<p>Confidential? – No</p> <p>n/a</p>
<p>Question 13: What media literacy tools and measures are available on your service?</p> <p>In particular, please provide any relevant information about:</p> <ul style="list-style-type: none"> • how you raise awareness of media literacy tools and measures on your service; • how you assess the effectiveness of any media literacy tools and measures provided on your service; and • how media literacy considerations, such as your users' ability to understand and respond to the 	<p>Confidential? – No</p> <p>n/a</p>

<p>content available to them feature in your thinking about how you design and deliver your services, for example in the user interfaces, flagging content and use of nudges.</p>	
<p>Question 14: Do you publish transparency reports with information about user safety metrics?</p> <p>Please provide any specific evidence and examples of reports, information around the categorisation and measurements used for internal and external reporting purposes, and whether you have measures in place to report at country/ regional level and track performance over time.</p>	<p>Confidential? – No</p> <p>n/a</p>
<p>Question 15: What processes and procedures do you have in place to measure the impact and effectiveness of safety tools or protection measures?</p> <p>If not already captured elsewhere in your response, please provide information relevant to all of the measures listed above explaining:</p> <ul style="list-style-type: none"> • how you test and review user awareness and engagement with each measure (including any analysis or research that you would be willing to share with Ofcom); • how often policies and protection measures are reviewed, and what triggers a review; and • how you test the impact of policies on users and the business more generally, such as how you balance the costs and benefits of new tools. 	<p>Confidential? – No</p> <p>n/a</p>
<p>Question 16: How do you assess and mitigate the risk of inadvertent removal of legal or non-harmful content?</p> <p>In particular, please provide any information on:</p> <ul style="list-style-type: none"> • how freedom of expression is taken into account during this assessment; • how appeals are handled and what proportion are successful; and 	<p>Confidential? – No</p> <p>n/a</p>

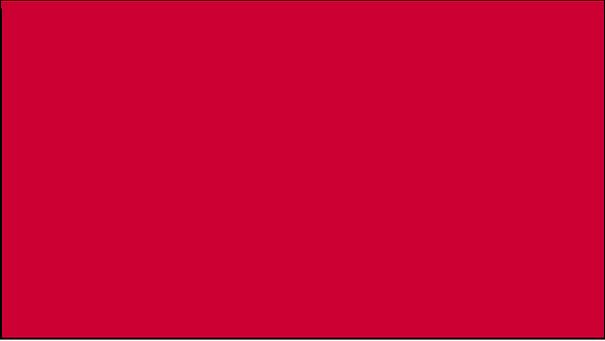
<ul style="list-style-type: none"> audits of automated removal systems and, if you have them, any metrics that relate to their effectiveness. 	
<p>Question 17: Have you previously implemented any measures which have fallen short of expectations and what was your response to this?</p> <p>Please provide evidence to support your answer wherever possible.</p>	<p>Confidential? – No</p> <p>n/a</p>
<p>Question 18: How does your service develop expertise and train staff around different types of harm? (e.g. do you have any partnerships in place?)</p>	<p>Confidential? – No</p> <p>n/a</p>

Questions for all stakeholders	Your response
<p>Question 19: What examples are there of effective use and implementation of any of the measures listed in article 28(b)(3) the AVMSD 2018?</p> <p>The measures are terms and conditions, flagging and reporting mechanisms, age verification systems, rating systems, parental control systems, easy-to-access complaints functions, and the provision of media literacy measures and tools. Please provide evidence and specific examples to support your answer.</p>	<p>Confidential? – No</p> <p>AV can and should be provided to the only recognised standard for age checking, BSI PAS 1296:2018. This ensures that age checks are carried out to a specified Level of Assurance (known in the standard as “vectors of trust”). The level can be chosen commensurate with the risk of harm. This choice can be made by the age-restricted information society service (ISS) itself, or imposed by regulations or agreed industry standards.</p> <p>AV providers can be subjected to audit and provided with certification against relevant standards, such as PAS1296, ISO27001 and as the ICO begins to approve assurance schemes, GDPR, building trust in their capability to protect personal data. We are designing the first GDPR assurance scheme in this field.</p>
<p>Question 20: What examples are there of measures which have fallen short of</p>	<p>Confidential? – No</p>

<p>expectations regarding users' protection and why?</p> <p>Please provide evidence to support your answer wherever possible.</p>	
<p>Question 21: What indicators of potential harm should Ofcom be aware of as part of its ongoing monitoring and compliance activities on VSP services?</p> <p>Please provide evidence to support your answer wherever possible.</p>	<p>Confidential? – No</p>
<p>Question 22: The AVMSD 2018 requires VSPs to take appropriate measures to protect minors from content which 'may impair their physical, mental or moral development'. Which types of content do you consider relevant under this? Which measures do you consider most appropriate to protect minors?</p> <p>Please provide evidence to support your answer wherever possible, including any age-related considerations.</p>	<p>Confidential? – No</p> <p>We do not express a view on what content should fall into this category. But there will be content which poses sufficient risk of harm to minors that effective age verification will be required. Where this is the case, that should be carried out;</p> <p>1 – to an agreed standard (PAS 1296:2018 is currently the best we are aware of)</p> <p>2 – independently of the VSPs; they have a strong vested interest in allowing users to access their sites, and their customers may not wish to disclose the amount of personal data required for an age verification check to such sites which may not be audited and certified for their data privacy and security measures.</p> <p>3 – independently of large platforms; becoming the gateway to users of a particular age would further entrench the dominant market positions of leading platforms; they may also set their own de facto standards for AV; and those standards may be influenced by their vested interest in maximising the number of users eligible to access age-restricted sites and advertising.</p> <p>4 – by a self-regulated sector benefiting from earned recognition by the regulator that its standards meet the minimum legal requirements, with the public trust that such an approach will engender.</p>

	<p>In addition, this should all take place within the UKAS structure for audit, certification and assurance, to maintain high standards, appropriate to the risk of each use case</p>
<p>Question 23: What challenges might VSP providers face in the practical and proportionate adoption of measures that Ofcom should be aware of?</p> <p>We would be particularly interested in your reasoning of the factors relevant to the assessment of practicality and proportionality.</p>	<p>Confidential? – No</p> <p>The regulator should issue some guidance to provide a degree of uniformity when sites undertake risk assessments. Without this, competitive pressures will also tend towards a race to the bottom in the level of risk assessed. Thus, where readily available and already accepted industry standards such as BBFC ratings can be applied, the regulator should offer some guidance linking the two regimes. For example, if a site hosts 18 rated films, it should be applying age verification rather than weaker age assurance, but that AV need not be to the highest level of assurance which might be applied to, say, knife sales.</p>
<p>Question 24: How should VSPs balance their users’ rights to freedom of expression, and what metrics should they use to monitor this? What role do you see for a regulator?</p>	<p>Confidential? – No</p> <p>n/a</p>
<p>Question 25: How should VSPs provide for an out of court redress mechanism for the impartial settlement of disputes between users and VSP providers? (see paragraph 2.32 and article 28(b)(7) in annex 5).</p> <p>Please provide evidence or analysis to support your answer wherever possible, including consideration on how this requirement could be met in an effective and proportionate way.</p>	<p>Confidential? – No</p> <p>n/a</p>

<p>Question 26: How might Ofcom best support VSPs to continue to innovate to keep users safe?</p>	<p>Confidential? – No</p> <p>Innovation in the age verification sector will be best supported by a stable regulatory regime which is based on widely applied standards such as BSI PAS 1296. This will unlock investment in technology to improve convenience to the user, reduce cost and improve quality.</p>
<p>Question 27: How can Ofcom best support businesses to comply with the new requirements?</p>	<p>Confidential? – No</p> <p>It is also important to be clear that there is a level playing field from the outset. Risk-based regulatory enforcement action can target larger operators, leaving smaller sites with a competitive advantage until they appear on the regulator’s radar screen. A strong monitoring regime will be required to identify VSPs who are not compliant before their competitors lose faith in the regulatory regime.</p> <p>Audit and certification will work well to raise standards amongst those minded to be compliant so should be encouraged.</p>
<p>Question 28: Do you have any views on the set of principles set out in paragraph 2.49 (protection and assurance, freedom of expression, adaptability over time, transparency, robust enforcement, independence and proportionality), and balancing the tensions that may sometimes occur between them?</p>	<p>Confidential? – No</p> <p>Protection and assurance.</p> <p>The quickest win in respect of VSPs is to protect minors from content rated 18 or above, and its equivalent in non-rated content. There is already a viable market in independent, standards-based age verification to enable this to be implemented from day one of the new legislation coming into force.</p> <p>The next step would be more graduated age-gating in line with the age-ranges set out by the ICO in the Age Appropriate Design Code. This</p>



would then be a strong foundation for a joined up approach to online harms that aligns data protection requirements with the requirements arising from the duty of care.