Your response

Questions for industry	Your response
Question 1: Are you providing a UK-established service that is likely to meet the AVMSD definition of a VSP? **Please provide details of the service where relevant. The establishment criteria under the AVMSD are set out in annex 5.**	Confidential? – No No
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?	Confidential? – No n/a
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) **In particular, please provide information explaining:** • **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.**	Confidential? – No n/a
Question 4: How are your Ts&Cs (or community standards/ acceptable use policies) implemented?	Confidential? – No n/a

In particular, please provide information explaining: • **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.**	
Question 5: Does your service have advertising rules? **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.**	Confidential? – No n/a
Question 6: How far is advertising that appears on your service under your direct control, i.e. marketed, sold or arranged by the platform? **Please provide details of how advertising is marketed, sold and arranged to illustrate your answer.**	Confidential? – No n/a
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?	Confidential? – No n/a
Question 8: Does your service have any reporting or flagging mechanisms in place (human or automated)? **In particular, please provide information explaining:**	Confidential? – No n/a

• **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.**	
Question 9: Does your service allow users to rate different types of content on your platform? **Please provide details of any rating system and what happens as a result of viewer ratings.**	Confidential? – No n/a
Question 10: Does your service use any age assurance or age verification tools or related technologies to verify the age of users? **In particular, please provide information explaining:** • **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**	Confidential? – No Our members provide age assurance tools including age verification.

restricting specific content to specific users), how this works.	
Question 11: Does your service have any parental control mechanisms in place? **In particular, please provide information explaining:** • **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.**	Confidential? – No We note the requirement under the Data Protection Act 2018 (GDPR) that where permission is relied on to process data, children under 13 cannot give such permission without parental consent. Therefore, as age assurance is applied across VSPs, there will be a consequential need to secure parental consent when the user is deemed to be under 13. It is likely therefore that these two functions will develop in parallel. This is of additional importance for film content, where the concept of "parental guidance" will require a link to be made between the child and their parent and legal guardian. Due to the lack of readily available data on such relationships, it is necessary to secure from adults once verified themselves, details of any children for whom they are responsible, so when those children seek to open accounts or watch PG rated material, their parents can be contacted for permission or kept informed. Age assurance will therefore be required for any user who attempts to watch content unsuitable for children under 13. Where that content presents a higher risk of harm, robust, independent, standards-based age verification will be required.
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. **In particular, please provide information explaining:** • **any time limits for dealing with complaints;**	Confidential? – No n/a

• 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.	
Question 13: What media literacy tools and measures are available on your service? **In particular, please provide any relevant information about:** • 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 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.	Confidential? – No n/a
Question 14: Do you publish transparency reports with information about user safety metrics? **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.**	Confidential? – No n/a
Question 15: What processes and procedures do you have in place to measure the impact and effectiveness of safety tools or protection measures? **If not already captured elsewhere in your response, please provide information relevant to all of the measures listed above explaining:**	Confidential? – No n/a

• 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.	
Question 16: How do you assess and mitigate the risk of inadvertent removal of legal or non-harmful content? **In particular, please provide any information on:** • how freedom of expression is taken into account during this assessment; • how appeals are handled and what proportion are successful; and • audits of automated removal systems and, if you have them, any metrics that relate to their effectiveness.	Confidential? – No n/a
Question 17: Have you previously implemented any measures which have fallen short of expectations and what was your response to this? **Please provide evidence to support your answer wherever possible.**	Confidential? – No n/a
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?)	Confidential? – No n/a

Questions for all stakeholders	**Your response**

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? **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.**	Confidential? – No Age Verification ("AV") systems are widely in use today for the purchase of age-restricted goods such as alcohol or fireworks, and access to age-restricted content such as gambling. Technology has also been ready to provide anonymised age verification since the original implementation data for Part 3 of the Digital Economy Act, Easter 2019. AV is provided using a variety of methodologies. It 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. 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. Weaker forms of age assurance may still be appropriate for lower risk content if a VSP is confident it will not be .
Question 20: What examples are there of measures which have fallen short of expectations regarding users' protection and why? **Please provide evidence to support your answer wherever possible.**	Confidential? – No
Question 21: What indicators of potential harm should Ofcom be aware of as part of its ongoing monitoring and compliance activities on VSP services? **Please provide evidence to support your answer wherever possible.**	Confidential? – No Unless OfCom wishes to duplicate the work of the British Board of Film Classification, or to add another layer of risk assessment to the BBFC certification process, then the logical measure of harm is the extent to which

	children below the BBFC certified age for content are viewing it. Applying an equivalent approach to classifying content not rated by the BBFC, including User Generated Content, or to reporting content which is not rated but should be classified as age-restricted will be necessary to ensure a comprehensive rating system, to which child protection measures can be applied. OfCom can then measure the effectiveness of those mechanisms in preventing children below the certified age accessing content.
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? **Please provide evidence to support your answer wherever possible, including any age-related considerations.**	Confidential? – No 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; 1 – to an agreed standard (PAS 1296:2018 is currently the best we are aware of) 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. 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. 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.

Question 23: What challenges might VSP providers face in the practical and proportionate adoption of measures that Ofcom should be aware of? **We would be particularly interested in your reasoning of the factors relevant to the assessment of practicality and proportionality.**	Confidential? – No We support the twin principles of practicality and proportionality. We would like to make clear that standards-based age verification is widely available, simple to apply, and delivered cost-effectively through an open and competitive market. As the proportion of the population who have already completed an age verification process increases, fewer such checks will be required as those customers are recognised by AV providers and need not re-verify. As a sector, we are developing protocols for interoperability so a customer can be recognised by one AV provider as having been checked by another already. The cost of AV checks is therefore already shared across multiple clients, and market forces will bear down on pricing, so cost should not be considered a prohibitive factor to applying age verification. We do not express a view on what level of age assurance is appropriate for any given content, but reiterate that where there is a risk of harm to minors of certain age-groups, then only age verification conducted independently to an agreed standard (PAS1296) should be considered sufficient in the higher risk cases. The technology and market to deliver it effectively and efficiently is now sufficiently mature that there is no need to rely simply on users entering their age or date of birth, or on the use of weaker assurance techniques such as social proofing in high risk situations. It should also be considered that the use of children's data where they are under 13 to conduct algorithmic age assurance may itself breach the Data Protection Act 2018, or at least cause compliance difficulties and costs for sites which are then potentially processing children's

	personal data. By outsourcing age assurance to age verification providers, even at the lowest levels of assurance, websites need never process children's data if they prefer not to. While we have no view ourselves on which forms of content merit the highest levels of age assurance provided by age verification, our experience is that content owners will tend to under-rate the level of risk, or base it on what they expect or hope their site to publish not what is actually found on their site in reality. 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.
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?	Confidential? – No n/a
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). **Please provide evidence or analysis to support your answer wherever possible, including**	Confidential? – No n/a

consideration on how this requirement could be met in an effective and proportionate way.	
Question 26: How might Ofcom best support VSPs to continue to innovate to keep users safe?	Confidential? – No 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.
Question 27: How can Ofcom best support businesses to comply with the new requirements?	Confidential? – No Critical to manage expectations. Technology is not infallible so the new regulatory regime should be described cautiously – e.g. "it will prevent minors stumbling across inappropriate content without any protective measures being applied to reduce the risk that they are exposed to such material" 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.
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	Confidential? – No **Protection and assurance.** 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,

balancing the tensions that may sometimes occur between them?	standards-based age verification to enable this to be implemented from day one of the new legislation coming into force. 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 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. **Freedom of expression** We support freedom of expression, and by applying effective protections for minors, the freedom of adults can be maintained. Age verification is the foundation of this by allowing us to distinguish between adults and children online. **Adaptability over time** The scope of the regime will need to be kept under review, as operators may adjust their business model to avoid falling within it. That said, it is unhelpful if the regulatory goalposts move too frequently. This can be avoided by consulting informally and formally prior to the launch of regulations, particularly with subject matter experts who might spot flaws that have gone unnoticed. We do not expect OfCom would make this mistake given its experience in regulation. The sophistication of existing technology already in use across the digital economy should not be underestimated when determining how high to set the bar at the start of the new regime. It is not supportable to argue, for example, that robust AV to a defined standard is not yet possible. **Transparency.** The regulator should also be able to inspect the operation of AV providers. This should be a last resort, with self-regulation, audit, certification and assurance schemes being the preferred mechanism for maintaining the rigour of AV.

	Robust enforcement, 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. We strongly recommend that the enforcement mechanisms in Part 3 of the Digital Economy Act 2017 are provided to OfCom to give it the capability to enforce on a global basis. These included blocking access to the sites (which we emphasise is possible even when VPNs or DNS over HTTPS technology is deployed) and blocking access to ancillary services such as payment and advertising networks, across all sites in a corporate group. **Proportionality** Age verification is not a huge step. It has been a requirement for adult 'cable TV' channels for over a decade, and has become easier to deploy ever since it was introduced. It can be anonymised; it does not require full identity to be disclosed. It is not a barrier to entry as the vibrant online vaping product market evidences.

Please complete this form in full and return to VSPRegulation@ofcom.org.uk.