Your response

Please refer to the sub-questions or prompts in the Annex of our Call for Evidence.

Question	Your response
Question 1: Please provide a description introducing your organisation, service or interest in Online Safety.	YourDataKey provides a real-time, verified Digital Identity controlled and used by citizens in all virtual and most physical situations – included in this verified Digital Identity are 'characteristics' such as DOB, Residency status, home address, gender, etc., – the Digital Identity provides the appropriate response to threshold challenges (such as age, location etc) from organisations, platforms, networks and e-tailers
Question 2: Can you provide any evidence relating to the presence or quantity of illegal content on user-to-user and search services?	No
Question 3: How do you currently assess the risk of harm to individuals in the UK from illegal content presented by your service?	YourDataKey doesn't assess the risk of harm to individuals, it removes the risk of harm caused by them inappropriately accessing regulated content, product and services
Question 4: What are your governance, accountability and decision-making structures for user and platform safety?	Not Applicable
Question 5: What can providers of online services do to enhance the clarity and accessibility of terms of service and public policy statements?	By upgrading the current 'tick-box' self-certification and replacing it with the requirement to present approved Digital credentials before progressing with the service the provider removes that potential for harm from say underage access, etc
Question 6: How do your terms of service or public policy statements treat illegal content? How are these terms of service maintained and how much resource is dedicated to this?	Not Applicable
Question 7: What can providers of online services do to enhance the transparency, accessibility, ease of use and users' awareness of their reporting and complaints mechanisms?	A good Web Portal by design will signpost this

Question 8: If your service has reporting or flagging mechanisms in place for illegal content, or users who post illegal content, how are these processes designed and maintained?	Not Applicable
Question 9: If your service has a complaints mechanism in place, how are these processes designed and maintained?	Not Applicable
Question 10: What action does your service take in response to reports or complaints?	Not Applicable
Question 11: Could improvements be made to content moderation to deliver greater protection for users, without unduly restricting user activity? If so, what?	Yes – starting with controlling the access to regulated content, products and services via Digital Identity; then apply the same traceable Digital Identity to posters of content, ensuring that whilst privacy is maintained they cannot hide behind anonymity if they break the law
Question 12: What automated moderation systems do you have in place around illegal content?	Apply the same traceable Digital Identity to posters of content, ensuring that whilst privacy is maintained they cannot hide behind anonymity if they break the law
Question 13: How do you use human moderators to identify and assess illegal content?	Not applicable
Question 14: How are sanctions or restrictions around access (including to both the service and to particular content) applied by providers of online services?	Not Applicable
Question 15: In what instances is illegal content removed from your service?	Not Applicable
Question 16: Do you use other tools to reduce the visibility and impact of illegal content?	Not Applicable
Question 17: What other sanctions or disincentives do you employ against users who post illegal content?	Not Applicable

Question 18: Are there any functionalities or design features which evidence suggests can effectively prevent harm, and could or should be deployed more widely by industry?	The full deployment of real-time Verified Digital Identity will stop inappropriate access to potentially harmful-but-legal content The removal of anonymity allowing 'posters' of illegal content to 'hide' by the full deployment of real-time verified Digital Identity
Question 19: To what extent does your service encompass functionalities or features designed to mitigate the risk or impact of harm from illegal content?	In the context of Verified Digital Identity – we stop inappropriate access to regulated content and make it difficult for 'bad-actors' to post abusive and illegal content with impunity
Question 20: How do you support the safety and wellbeing of your users as regards illegal content?	By making sure that the 'posters' of illegal content have to use a verified Digital Identity before posting or commenting, we remove anonymity and therefore establish traceability enabling the relevant authorities to act against the provider
Question 21: How do you mitigate any risks posed by the design of algorithms that support the function of your service (e.g. search engines, or social and content recommender systems), with reference to illegal content specifically?	Not Applicable
Question 22: What age assurance and age verification technologies are available to platforms, and what is the impact and cost of using them?	While there are legacy analogue services and AI interpretation of facial features- these are already proven to be easily abused YourDataKey uses real-time blockchain/DLT technology to provide e-commerce friendly age assurance and verification; evidencing the verification by storing a time and date stamped PDF of the transaction
Question 23: Can you identify factors which might indicate that a service is likely to attract child users?	Not our area of expertise – we stop child users having inappropriate access
Question 24: Does your service use any age assurance or age verification tools or related technologies to verify or estimate the age of users?	Yes - YourDataKey uses real-time blockchain/DLT technology to provide e-commerce friendly age assurance and verification; evidencing the deployment of such verification by storing a time and date stamped PDF of the transaction
Question 25: If it is not possible for children to access your service, or a part of it, how do you ensure this?	Implicit to the establishment of the child's verified Digital Identity

Question 26: What information do you have about the age of your users?	DOB – verified by multiple independent trusted data-sources
Question 27: For purposes of transparency, what type of information is useful/not useful? Why?	Citizen provided personal data – is verified by multiple independent trusted data-sources, with the citizen's approval
Question 28: Other than those in this document, are you aware of other measures available for mitigating risk and harm from illegal content?	There are many 'coping' measures – none of which have the precision provided by deploying verified Digital Identity – Prevention is better than cure

Please complete this form in full and return to OS-CFE@ofcom.org.uk