

Sent via email: IHconsultation@ofcom.org.uk

23 February 2024

Dear Sir/Madam,

RE: Protecting people from illegal harms online

FSB welcomes the opportunity to provide a response to the above consultation.

FSB is a non-profit making, grassroots and non-party political business organisation that represents members in every community across the UK. Set up in 1974, we are the authoritative voice on policy issues affecting the UK's 5.5 million small businesses, micro businesses and the self-employed.

Small businesses, unlike larger businesses, have fewer resources meaning that they are more likely to struggle to comply with new regulatory requirements. With that said, we do support the overall aim of the consultation in reducing illegal harms on users and in largely striking the right balance between risk and proportionality in the overall regulatory approach taken. We recognise that the regime is new and therefore we would welcome any issues to be ironed out with larger and high-risk services first, as well as guidance also updated on a regular basis, given lack of data and information on the specific tools that services may use and how they may be able to adapt their technology to comply with the regime.

Almost two-thirds (62%) of small businesses in our research cite the current domestic regulatory environment to be more of a burden than a benefit to their business.¹ With cumulative burden of regulation continuing to be a challenge for small businesses, we welcome clear and concise guidance, with illustrative examples to help them comply with any new requirements. It would also be helpful to reference existing requirements of other regulations such as data protection which small businesses are likely already complying with where requirements are the same or similar to help reduce the compliance burden.

We have not commented on every section within the consultation, only those that are directly to small businesses.

Volume 3: How should services assess the risk of harms?

Governance and accountability

We recognise the importance of governance and accountability arrangements in organisations being appropriately set so that they help to prevent risk of harm to individuals. We welcome that smaller services in most cases will only need to name a person accountable to the most senior governance body, and that for proportionality most measures only relate to large or multi-risk services. We believe

¹ FSB report, Escaping the Maze: How small businesses can thrive under the British Columbia regulatory model, 2021, <https://www.fsb.org.uk/resource-report/escaping-the-maze.html>

that this approach is proportionate to the risk of harm. It is worth noting that in most cases for small and micro businesses, whether low or multi-risk, this is likely to be the business owner, and therefore, this should be clearly communicated to them together with their responsibilities according to the risk of harm.

For small multi-risk services, we would like to see appropriate guidance published following the relevant codes of practice to help manage risks appropriate to their size and impact on users, including on the extent of the risk of harm. In terms of identifying whether a small business is a multi-risk service, the assessment is obvious if it is known that there is history of prior occurrences on the service, however, if a service has not experienced any harms or incidents it could in some circumstances be difficult to identify whether it is likely that these could occur even with appropriate mitigations in place. Greater clarity would help small businesses avoid getting expensive external advice in helping to identify harms.

Services' risk assessment

We believe that risks assessments are a good way to identify and manage risks for businesses, and the proposal that they should be carried out at least once a year or once a significant change occurs would be suitable, as this is in line with other regulations such as that on data protection. However, saying that, while we believe that they should be flexible enough for businesses to fulfil their legal obligations, the expectations in terms of detail, procedures and processes outlined should be reflective of business size and risk. We appreciate inclusion of clear and targeted recommended actions and assurance that the risk assessment duties can be implemented in proportionate way for all services. Small and micro businesses are less likely than larger services to have access to more sophisticated tools to assess, manage and mitigate risks, and they should be able to reflect this in the risk assessment. Consideration should be given to numbers of users, types and extent of harm and steps a business is able to take to mitigate them and where these obligations could be absorbed into existing practices for compliance or existing systems that they may have. Where possible, Ofcom should consider appropriate tools to help businesses to customise their approach to risk assessments similar to that of data protection impact assessment guidance that the ICO produces, including checklists and relevant examples.

Record keeping and review

We agree that there should be some record keeping, and we would also suggest that businesses should be able to adapt this obligation to their risks, provided that they have the appropriate guidance and tools to facilitate that adaptation. Similarly to the points raised above, if record keeping requirements are in line with existing protection legislation, then this would help to alleviate some burdens for businesses, provided that this is made clear in the guidance and examples.

We understand that Ofcom is not currently proposing to exercise the power to exempt specific services from record keeping and review duties, which is understandable given that this is a new regime and there is little data on the types of services that would benefit from this. However, we would like to highlight that it would help to alleviate some burden if record keeping and review issues were firstly ironed out in relation to implementation by larger and high or multi risk services before they are imposed on lower risk services – i.e. a staggered approach in implementation. We would like to see risk based and service specific guidance, with clear examples and expectations clearly set out.

Volume 4: How to mitigate the risk of illegal harms – the illegal content Codes of Practice

It is positive to see that the consultation's aim in mitigation of harms is not a one size fits all approach and that implementation will be largely applied to services with greater harm and risk levels, given the costs associated with compliance.

Content moderation (user-to-user)

We recognise that most of the requirements are aimed at larger and multi-risk services, and agree that where possible all user-to-user services should have systems and processes in place to swiftly take down illegal content of which the service is aware. We would like to note with regard to small and micro businesses in particular, that this may mean that their systems and processes will not be at the same level of sophistication as those of larger services. This means that they will need greater support in relation to implementation and clear examples of best practice, so that cost-effective measures can be put in place, particularly for those that are lower risk.

We agree that where possible businesses should be able to adapt existing mechanisms, processes and policies to suit the characteristics and ability of a particular service. We appreciate the flexibility offered to businesses in making such arrangements particularly for those that are smaller/lower risk who are more likely to use human moderation to a greater extent than a larger ones, and we therefore, expect the guidance will help those businesses adhere to the requirements by making suitable adaptations.

Search moderation (Search)

As with content moderation, search moderation should also be proportionate to the service's own characteristics and ability, for example, where automated tools are not as widespread or are unavailable and the service relies on human review and reporting data. We recognise that all search services will be expected to de-index or down-rank illegal content which they are aware will appear in search results. We understand how this is critical to protecting users from harm, and that there is a no one size approach in terms of the methods used. More detail in the Codes and accompanying guidance will be welcome.

Reporting and complaints (U2U and search)

For any service operating online, user reporting and complaints processes should be key in ensuring user safety and fairness. We agree that all U2U and search services should have easy to use complaints processes and take appropriate action in response to complaints in relation to illegal content. However, we do have some concerns in terms of setting up an appeals process where content has been incorrectly identified, as small businesses have limited resources there should be guidelines on how this process could be handled efficiently, with a clear and easy to follow criteria set on handling appeals to avoid disproportionate impact on resources. Similarly, we would like to flag that acknowledging receipt of complaints, which may be automated, may take longer to set up if the systems do not allow doing so at present. We would also expect appropriate guidance to be shared which would indicate expected timeframes for a complaint response, or if not, give a clear steer about reasonable timeframes, particularly for smaller businesses taking into account their limited availability of resources.

Given that our recent research shows that 37 per cent of small businesses have suffered from fraud over the last two years, and 83 per cent of those say that they have experienced a financial cost following their most impactful fraud, we are supportive of greater action by larger platforms including collaboration with law enforcement.² This includes the proposal to establish and maintain a dedicated reporting channel for fraud for all larger services with a medium or high risk of fraud, for trusted flaggers such as HMRC, DWP and NCA etc to enable better engagement between expert third parties with the competence expertise and knowledge to detect and investigate fraud.

Terms of service and publicly available statements

It is sensible to assume that all U2U and search services should be able to include in their statements how individuals are protected from illegal content, as well as information on protective technology used for compliance with illegal content safety duties, and policies and processes that govern handling and resolution of relevant complaints. We agree that these should be clear and easy to find as well as navigate. However, as mentioned before, if these are similar to the format of data privacy statements then we would ask that Ofcom considers similar tools to that of privacy statement generators where businesses can input information to help them to be customised to their needs. This could help to alleviate any uncertainty as well as reduce some of the associated compliance burden.

User access to services (U2U)

We are supportive of the proposal to remove a user account from service if there are reasonable grounds to believe that is operated by or on behalf of terrorist groups or organisations proscribed by the UK Government. In this case, we believe that to prevent users getting classified in error, where there are automated systems they should be also reviewed through human interaction. However, if a breach is confirmed after a proper investigation and due process, it would be appropriate to ban usernames, emails and IP addresses where possible. It is likely that a username ban on its own or an email ban would not be a significant deterrent, so a combination of factors should be considered where possible. Consideration should also be given to usernames which remain available following association with certain banned groups, and the reputational impact on other users if that username becomes available and they unknowingly take it up.

Cumulative assessment

Overall, of the measures that are proposed for all services, we appreciate that the more onerous measures are for multi risk or larger services, meaning that the ability of small businesses to comply has to some extent been taken into account. We agree that it is possible that some services that are provided by small and micro businesses will identify multiple and significant risks and therefore will be required to take more significant measures. In this case, we would ask that Ofcom work with those small businesses to help them comply, consider the costs involved for them, and adopt a more staggered approach taking into account their immediate capabilities and what they can do over time.

² FSB report, Cracking the case: Uncovering the cost of small business crime, 2023, <https://www.fsb.org.uk/resource-report/cracking-the-case-uncovering-the-cost-of-small-business-crime.html>

Volume 5: how to judge whether content is illegal or not? (Illegal Content Judgements Guidance)

In most cases, it should be relatively clear what is illegal content and we would expect Ofcom to provide suitable guidance. In terms of 'reasonable grounds to infer', this is a much lower hurdle and very different to the 'beyond a reasonable doubt' threshold that is usually used in the criminal courts and, services may be free to take down content beyond what is illegal under the Act provided that it is in their terms of service. However, small businesses do need certainty around what the minimum requirements are and the steps that they need to take, so while some ambiguity or uncertainty may arise in respect of what goes beyond the requirements of the Act, we would expect the guidance to state clearly, with examples, how small businesses should apply the test of 'reasonable grounds to infer', so that they do not fall foul of the regulations, or mistakenly take-down content which is not infringing. We understand that the Act states that illegal content judgements are made on the basis of all relevant information that is reasonably available to the service provider taking into account the size and capacity of the provider and considerations such as user profile, activity and complaints. We agree that the guidance needs to be accessible to those with less legal expertise, and small businesses are unlikely to have this in-house. We would also suggest that the guidance needs to be as concise as possible given the high number of offences captured under the Act, with that if that is not possible, summaries should also be available. There may be instances where service providers are in dispute with their users' with regard to their content. It would be helpful for businesses to know what Ofcom expect of service providers in terms of extent of investigation and due process or complaints procedure in relation to content takedown disputes. As small businesses have limited resources, there needs to be a very expedited process for managing disputes and appeals and therefore, clarity on the exact criteria as well as supporting flow charts that can provide transparency on the process as well as any expectations would be welcome. There is at present a complete absence of cost-effective dispute resolution process in relation to issues between a service provider and user content provider, and businesses would welcome support by the regulator for such a process to be established.

Volume 6: Information gathering and enforcement powers, and approach to supervision

Information powers

We agree that that given the new regime there will be plenty of requirements for Ofcom to gather information to build evidence and appropriately exercise functions. In terms of information requests, we would like consideration to be given to allowing small businesses to respond to such requests before they bite, and for there to be a process of engagement to enable fair and reasonable requests to be addressed, and oppressive requests challenged. We would like to see the size of the business and its ability to comply taken into consideration. It would not be reasonable to expect a small business to gather information and respond to a request in a similar way to a large business, which may have a dedicated compliance team.

Enforcement powers

Given the seriousness of the harms involved, it is understandable that protection of users should be paramount. We ask that Ofcom works together with small businesses and helps them to comply where necessary, rather than following an enforcement approach from the outset. Initially, it maybe that

small businesses will be able to implement the simplest and easiest measures but struggle with those which are more onerous and costly/time consuming. It is positive and helpful to see that Ofcom is willing to look at what is reasonable on a case-by-case basis, and that likely enforcement will in the first instance be focused on the most serious and harmful risks and business.

Yours sincerely,

Neil Sharpley
Policy Champion, Ministry of Justice and Home Office Policy Units
Federation of Small Businesses

For further information please contact:

Kristina Grinkina
Kristina.grinkina@fsb.org.uk
Federation of Small Businesses
3rd Floor, 10 Dean Farrar Street, Westminster, SW1H 0DX