

ICO call for views: Data protection and content moderation.

The ICO is calling for views to support the development of guidance that will provide clarity on how data protection law applies to online content moderation processes.

Content moderation is the process of analysing content generated by users of online platforms to assess whether it meets certain standards or whether it is appropriate for a given context. This content can often include personal data and the analysis may trigger subsequent action to be taken, such as removal of the content, escalation to human moderator or application of a content warning. We have a role to ensure that personal data is processed in compliance with data protection law during content moderation.

This work is the first step in meeting commitments set out in our November 2022 [Joint Statement with Ofcom](#) to provide certainty for organisations in scope of the future UK online safety regime

Our guidance, in parallel with our ongoing collaborative work with Ofcom, will support organisations to meet both their data protection and online safety responsibilities. It will also support other organisations developing and deploying content moderation in a non-online safety context.

As part of our call for views we want to understand more about:

- How content moderation solutions use people's personal data, and how the solutions are being used or developed more generally
- Where clarification is needed on the application of UK GDPR, DPA 2018 and PECR to content moderation
- What challenges organisations are facing relating to data protection when they deploy content moderation processes

We recognise that content moderation is a developing area and new approaches are continuing to emerge. We are launching this call for views to develop our knowledge and to ensure that the guidance we provide about meeting data protection expectations is meaningful to organisations.

Responding to the call for views

We want to hear from organisations and individuals with expertise, experience or an interest in the use of content moderation technology.

Please complete the call for views through our online survey, available through this link: [survey link](#).

Alternatively you can download this Word document and email your response to onlinesafetyteam@ico.org.uk.

You don't need to answer every question - some of the questions may not be relevant to you or your organisation, so please skip these as necessary.

This call for views will remain open until **9 June 2023**.

If you have any general queries about the call for views or would like further information, please email us at onlinesafetyteam@ico.org.uk.

Privacy statement

For this consultation, we may publish a summary of the responses but will not publish the actual responses received from organisations or individuals. If we publish a summary of the responses, information and views will not be attributed to individual respondents.

Should we receive an FOI request for your response we will need to consider whether we make it available. However, at this point, we would always seek to consult with you for your views on the disclosure of this information before any decision is made.

For more information about what we do with personal data please see our [privacy notice](#).

Please note that we are using the platform Snap Surveys to gather this information. Any data collected by Snap Surveys for ICO is stored on UK servers. You can read their Privacy Policy at www.snapsurveys.com/survey-software/privacy-policy-uk/

Questions

About you

1. Are you answering this call for views as:

- A representative of an organisation that develops content moderation solutions for others to use
- A representative of an organisation that uses content moderation solutions developed by a third-party
- A representative of an organisation that develops content moderation solutions for use in-house
- A representative of an organisation that develops content moderation solutions for use in-house AND solutions for others to use
- Other (please specify in Q2)

2. If you selected 'Other' in the previous question, please pick one option:

- A representative of a professional, industry or trade association
- A representative of a third sector/civil society body (eg charity, voluntary and community organisation, social enterprise or think tank)
- A representative of a public body
- A representative of a private sector organisation
- An academic, academic research group or academic institution
- An individual acting in a private capacity (eg someone providing their views as a member of the public)
- Other (please specify)

3. What sector(s) is your organisation involved in? Tick all that apply.
(This question is for developers and/or users of content moderation systems only)

- Social media
- Forums or chatrooms
- Review sites
- Blogging

- Gaming
- Retail
- P2P marketplaces
- Volunteering
- Job searching
- Search engines
- Accommodation searching
- Adult entertainment

X Dating

- Crowdfunding or fundraising websites
- Content subscription or fansites
- Private messaging
- Video sharing or livestreaming

X Video calling

Other (please specify): Cryptocurrencies, Cyberlockers

4. For the content moderation solutions you develop for others to use, where are your clients based? Tick all that apply. (This question is for developers of content moderation systems for others to use only)

X UK

X Europe (excluding UK)

X Rest of the world (excluding UK and Europe)

5. How would you describe your organisation? (This question is for developers and users of content moderation systems only)

- 0 to 9 members of staff
- 10 to 249 members of staff
- 250 to 499 members of staff
- 500 or more members of staff
- Not applicable or not sure

6. What is the name of your organisation and your role (if applicable)?

Internet Watch Foundation (IWF), Head of Policy and Public Affairs

Content moderation overview

We are asking the following questions to improve our understanding of how content moderation systems work and challenges to their development and deployment

7. Please tell us about the content moderation systems you have used, developed or experienced.

We are interested in information including what technology is used, the purposes that content moderation serves, what areas of a service are moderated, the effectiveness of different approaches, and whether automation is combined with human moderation.

The Internet Watch Foundation is the UK hotline for the reporting and removal of child sexual abuse material. We receive reports of suspected child sexual abuse from members of the public and are one of only two hotlines globally permitted to proactively search for this material online.

We also provide technical tools and data sets that help platforms keep their platforms free of child sexual abuse material. We have over 180+ members from a range of sectors including social media, software development providers, domain name registries and registrars, payment providers, cryptocurrency providers, internet service providers, mobile network operators and we currently have working partnerships with Mindgeek, the world's largest provider of adult content and are exploring the possibility of working with subscription fan sites like OnlyFans.

We offer several data sets to our members in the sectors mentioned above and membership of the IWF is based on a sliding scale of fees based on sector, number of employees and revenue. The largest companies pay as much as £80,000 per year and the smallest as little as £1,000.

All the IWF's services are then available to members to deploy to assist in their content moderation of illegal child sexual abuse content. The IWF provides several lists of illegal content (specifically Child Sexual Abuse) which are outlined below, but any content that makes it onto the list has been categorised as either Category A, B or C content in line with the UK Council's Sentencing Council Guidelines (2014).

The services we offer are:

Webpage (URL) blocking: This service is a list of webpages we have confirmed as hosting child sexual abuse material. The best way of dealing with illegal content is to request its removal at source, but whilst we are waiting for content to be removed, (as it is mainly hosted outside the UK), we will add the webpage to our blocking list.

The list can be used to block access at network level, in filtering solutions and by search providers who can deindex these URLs, so they won't be returned in search results. The list is currently being utilised by a range of IWF members including internet service providers, filtering providers, search providers, internet security providers, hosting service providers, registrars and others involved in internet, communications, or network security.

In 2022, the total number of URLs included in our list was 230,922, a 14% increase on 2021's figures. On average, 1,029 URLs were added to the blocking list every day, and the list contained on average 11,488 URLs per day a 108% increase on 2021's figures.

The list is shared with service providers operating globally and in 2020, three mobile network operators and internet service providers serving the UK market, provided the IWF with information on the number of hits against our URL list which totalled 8.8 million attempts. These attempts cannot be attributed to individual users, as it could have been bots and crawlers hitting these pages, but it does demonstrate that there are a staggering number of attempts to access these pages displaying illegal content.

The URL list is subject to human review twice a day, once at the start of the day to assess whether the illegal content is still live or not, and once at the end of the day to ensure new URLs are added to the list. The list is a dynamic list, and these quality control checks ensure we are not over blocking access to potentially legitimate content that may have replaced illegal content previously hosted on the page once it has been removed.

You can read more about our URL list here:

<https://www.iwf.org.uk/our-technology/our-services/url-list/>

Hashes of known child sexual abuse- A “hash” is a unique code or string of letters and numbers generated from a binary picture. Hashes can automatically identify known child sexual abuse imagery without needing to examine each image individually. This can help to prevent the online distribution of this content if used in content moderation by providers of online services.

In 2022, the IWF curated 1.6 million quality assured hashes or digital fingerprints of unique child sexual abuse images and thanks to the work of our mapping tool, [Intelligrade](#), we have been able to detail more information about what is happening in each individual image, which enables companies to map these hashes to other standards of classifications across the five-eyes countries (UK, Canada, NZ, Aus and US) as well as the Interpol base line standard.

We provide our hash list in several formats including pDNA, MD5, SHA1 to our members.

The Hash list can be utilised by the IWF’s membership and is mainly applicable to hosting or file sharing sites, social media and chat services, data centres and search engines.

Further information about our hash list is available on our website: <https://www.iwf.org.uk/our-technology/our-services/image-hash-list/>

Keywords list: The IWF provides a list of keyword terms known and associated with the distribution of child sexual abuse material, or phrases used by paedophiles to locate such content online.

We have over 8,000 keyword terms that are available to our industry members, that is reviewed monthly and quality assured. These keywords are mainly used by gaming providers, forums, social media providers, search engines and in checking files or domains that may contain criminal content the needs further investigation.

We also use keyword search terms in a project in partnership with Mindgeek and the Lucy Faithful Foundation, which sees a [chatbot](#) deployed on the Mindgeek owned site, Pornhub. This is deployed when a UK based user searches for one of the 28,000 keywords (IWF and Mindgeek provided lists) that may link through to child sexual abuse material and provides those trying to use these terms with the opportunity of engaging with providers who can assist them with their

behaviour before potentially going down a pathway to viewing illegal child sexual abuse imagery.

In the first month the chatbot was deployed, the chatbot was deployed on 175,000 occasions.

The IWF also offers a range of other services to its members including [virtual currency alerts](#), [simultaneous alerts](#) (US companies in scope of US mandatory reporting laws- meaning we notify NCMEC as well as the provider hosting content), [notice and takedown](#) (to UK based providers), [domain alerts](#), [payment brand alerts](#), [list and notifications to newsgroup providers](#). More details on all these services are available on the hyperlinks provided.

8. What do you consider to be the main challenges to development and deployment of content moderation solutions?

Encryption: We have been consistently raising concerns about the impact of encryption on the deployment of all the services mentioned above. Large social media platforms are proposing to End-to-End Encrypt their private messaging functions, which would mean, that at present, there is no way technically for a service provider to utilise any of the content moderation tools we provide in those environments.

We have been working in partnership with the UK Government, through its safety tech challenge funds to explore what the possibility could be of preserving user privacy, whilst detecting content entering or leaving End-to-End Encrypted environments and have been working with our members Cyacomb in the development of a contraband filter which could be compatible with preventing known material entering or leaving these environments.

We have also been working with another of our members, Safe to Net, to develop an application that could be installed, voluntarily, on the devices of individuals who are at risk of accessing child sexual abuse material. Development of this application is ongoing and brings together experts from across the UK and EU over the next two years to develop the application, thanks to 2 million euros of EU funding.

We have also previously raised concerns about the impact of DNS over HTTPS within the technical standards community at the Internet Engineering Taskforce (IETF). We are concerned that if companies don't

implement new technical standards around browsers and applications with due regard to child safety online, that parental controls, traditionally deployed at Internet Service Provider level and other filtering mechanisms such as the IWF's blocking list will be circumvented and therefore both children and adult consumers will be at further risk of seeing content that is not age appropriate and in the worst-case illegal. Another major concern is that if these updates are released in new browser developments, that these changes could happen without the consent of the end user or without them knowing that controls that they have established have been overridden. This is particularly applicable to Apple's Private Relay and Google Chrome who have both made attempts to implement the new DoH standard and have had to further consult with IWF on how we ensure that sufficient safety mechanisms remain in place.

Whose responsibility, is it? This brings us on to the next debate about who is responsible and who should be acting and at what level of the internet infrastructure stack.

The current focus of Government legislation is on platforms, providers of user-to-user services and search services. Traditionally, Internet Service Providers have been relied upon by Governments to deploy IWF services and parental controls, but a shift in their control or role as gatekeepers to the internet has seen Government begin to look elsewhere to improve the response to child sexual abuse online.

The further down the internet ecosystem you go, the hard it is to act. Once you are down to Domain Name providers and Registries and Registrars the only action, they can take is to suspend a whole domain, which depending on the size of the service they are dealing with is a fairly blunt instrument. That does not mean to say, there are not steps that they can take.

We have also seen in debates around the online safety bill, platforms attempting to shift the responsibility on to app stores to verify the age of their users before the applications are downloaded. Whilst supportive of stronger age verification measures online, and children having age-appropriate experiences and applications stores have a part to play in that process, it shouldn't be an obligation placed solely on app stores at the expense of protections in applications too.

Artificial Intelligence- In the past few months, we have also been seeing content that has been created through Artificial Intelligence. We have received a small number of anonymous reports from members of

the public and actioned a small number of URLs containing this material. Some of this content has been Category A material and of children in the 0-2 age range. This material is now so realistic that IWF analysts would struggle to tell the difference between a computer-generated image and that of a real child. These images can be created incredibly quickly, and whilst their current creation and distribution is not high in terms of numbers, it is an emerging threat that we must be aware of in the future. We know that offenders are exchanging information about how these images can be created in forums and are using older forms of technology to distribute and share the images they have created.

Data protection

We are asking these questions to improve our understanding about the data protection risks and challenges associated with content moderation, and any uncertainties that exist in this area.

- 9.** What do you perceive to be the main data protection risks and challenges associated with the development and deployment of content moderation systems?

The IWF must ensure that any companies accessing, downloading and deploying our services are legitimate companies and that they commit to handling the data we provide in line with strong data protection standards. They are required to sign strict licensing agreements and our membership team ensure that there is a due diligence exercise before membership is agreed between the company requesting to join and the IWF.

This includes the company providing information on the sector they operate in, addresses for where they are physically located and provide names and contact details of their employees responsible for the integration and deployment of services and a Primary Contact.

In 26 years of gathering information from public reports, proactive searches and sharing that data with industry, there has not yet been a single identified breach in the sharing of this information.

- 10.** Please list any particular areas of uncertainty where clarification is needed in the application of data protection law (the UK GDPR and the DPA 2018) and/or the Privacy and Electronic Communications Regulations to content moderation.

One of the biggest concerns to the IWF currently, surrounds the implementation of EU law on content moderation practices in companies. We currently have a situation in Europe, where we have [a temporary derogation from the e-privacy directive](#). This was secured on 6 July 2021, and lasts for a period of three years, giving companies a clear legal basis to take voluntary actions to detect, remove, report, and block access to child sexual abuse material on their services. It took quite some time to negotiate this position in Europe and the temporary derogation was a result of unintended consequences to email and messaging services being brought into scope of e-privacy legislation through the passage and implementation of the electronic communications code.

In the six months it took to agree the temporary derogation, one company took the decision to stop scanning to detect child sexual abuse material in those environments. According to data submitted to the National Center for Missing and Exploited Children (NCMEC), [there was a 58% reduction in reports](#) of child sexual abuse material from European Union Member States. The European Commission has now released a proposal for a regulation: [Laying down new rules to prevent and combat child sexual abuse](#) which seeks to move from a system of voluntary detection, to one where companies are required to detect child sexual abuse. It is important to the IWF, that this legislation provides clear legal certainty to companies to continue detecting child sexual abuse material in all its forms so that detection can continue, and child sexual abuse can be detected wherever it is uploaded to a platform, be that in public parts of a platform, private messaging or in email communications.

We should be clear that the situation in the UK is slightly different to that in Europe. In the UK, the Government confirmed in response [to a letter from the Chairman of the European Scrutiny Committee](#) in 2020, that the UK was confident companies could continue to detect child sexual abuse despite messaging and email services being brought within the scope of the electronic communications code, for three reasons:

1. There are several offences which criminalise CSEA activity.
2. There are separate legislative arrangements that govern the monitoring of content of communications and the collection of communications data that are relevant.

3. The Investigatory Powers Act (2016) provides several grounds under which companies may monitor the content of communications for the detection of CSEA.

It is our understanding that the temporary derogation does not apply in the UK, as this became law post Brexit, and the above confirmation from the UK Government was sufficient for companies to continue to detect on a voluntary basis because of this response from the Home Office in 2020.

Where further guidance could be needed is on whether the current legislative frameworks provided for above and with the Online Safety Bill making it onto the statute books requires companies to detect in End-to-End Encrypted environments, beyond Ofcom issuing a “use of technology notice” under Section 110 (Notices to deal with Terrorism or CSEA Content) of the Online Safety Bill¹ currently before Parliament.

Another challenge with the Privacy in Electronic Communications Regulation is that, currently, detection within these environments can only be performed with user consent. Our understanding is, [given the advice the ICO](#) issued during the UK Government’s Safety Tech Challenge Fund, that in order for scanning to be performed in an End-to-End Encrypted environment messaging environment, it would have to meet a higher threshold, than simply ticking a box as part of terms and conditions or having boxes pre-ticked as part of the sign-up process. The obvious flaw in this, is that paedophiles or those creating, distributing or wanting to receive illegal indecent images of children, would obviously not permit their applications to be scanned for this content.

The Privacy in Electronic Communications does allow for some exemptions that are strictly necessary for delivering a service legally and once the Online Safety Bill has been passed in the UK, it is understood that technologies in this space could be deployed, but greater guidance from the Digital Regulation Cooperation Forum (DRCF) on how the UK regulators plan to address this issue would be gratefully received by those seeking to protect children.

Information gathered and used

¹ <https://bills.parliament.uk/publications/49376/documents/2822>

We are asking these questions to improve our understanding of what information is used in content moderation systems.

Please answer the following questions in relation to a content moderation system that you have used or developed most often or most recently.

The questions in this section are for developers and/or users of content moderation systems only.

11. Does the content moderation system you have used or developed require data sets for training and/or testing?

- Yes
- No
- Unsure/ not applicable

If yes, please provide information about from where this data is sourced

We provide the data sets that companies use in their content moderation systems. We source this data from reports we receive from members of the public who have stumbled across child sexual abuse online, and we have confirmed as containing child sexual abuse. We are also one of only two hotlines, globally, empowered to proactively search the open internet for child sexual abuse material. We have also recently commenced a programme of hash sharing, which has allowed us to extract 2 million Category A and B images from UK policing's Child Abuse Image Database (CAID) and we grade them and add them to the IWF's hash list to share with industry, to prevent these from circulating online.

12. Is the content connected with an individual service user's profile while it's being moderated?

- Yes
- No
- Unsure/ not applicable

Please provide more information

This is not relevant to us at IWF.

13. Are there policies and/or governance mechanisms around human moderators accessing information about individual service users?

Yes

No

Unsure/ not applicable

If yes, please provide more information

This isn't relevant to us at IWF.

14. Do the answers you've provided in this section differ across different systems you have used and/or developed? If so, how? across different systems? If so, how?

N/A

Provision of information to users

We are asking these questions to improve our understanding of what information is provided to individuals about content moderation.

If you are answering these questions as a developer or user of content moderation solutions, please answer in relation to a moderation system that you have used or developed most often or most recently.

15. Are individual service users made aware that content moderation is being used?

Yes

No

Unsure/ not applicable

If yes, how is this information given to them?

Companies that deploy IWF services are listed on the IWF website. Some will actively promote what services they deploy to protect children widely; others may wish to be more discrete about what services are deployed and where on their platforms.

Those that do communicate their involvement with IWF, will often do so through terms of service or at the point of sale (in the case of broadband providers for example, where they will talk about filtering and parental controls at set-up).

Providers of applications and browser services will often discuss moderation and terms of service once they are installed in a device, but with both broadband providers, mobile network operators and platforms, you will have to follow-up directly with those providers about the steps they take to inform their customers about the use of our data.

16. Is information given to individual users if action is taken on their content by a moderation system?

Yes

No

X Unsure/ not applicable

If yes, what information is given to users?

This is a question for individual platforms.

17. If you answered 'yes' in question 16, are there mechanisms in place for users to appeal against that action?

Yes, if an individual reporting suspected child sexual abuse is unhappy with the determination we make, appeals can be submitted to us using a feedback form. Similarly, companies who deploy our services can also question the inclusion of a link or an image in our services and follow the same appeals process as individual reporters.

In the first instance, any request for review goes to our Hotline Director, who will make the first determination on whether to uphold any appeal. Ultimately, if the person appealing remains unsatisfied with the answer they receive, it is then referred to the relevant lead policing agency for a final decision. The IWF's Board is also kept informed of any assessment decision that is made by a relevant lead policing agency which would reverse a decision made by the IWF.

Full details on our complaints and appeals process is available [here](#).

Reporting

We are asking these questions to improve our understanding about reporting mechanisms, including how information about individuals is used in content reporting.

If you are answering these questions as a developer or user of content moderation solutions, please answer in relation to a moderation system that you have used or developed most often or most recently.

18. Do mechanisms exist for individual service users to report content?

Yes

No

Unsure/ not applicable

If yes, how does this work and what action is taken when a report is made?

People reporting to the Internet Watch Foundation have the option of leaving contact details so that we can inform them on what action has been taken on their report. They are also given the option of not providing their details and can report to us securely and anonymously via our website.

If reporters have left contact details, we will notify them via email within 24 hours on the outcome of their report.

With Report/Remove, we enable children and young people to self-refer images they may have generated themselves. In this process, we require children to have a way of being contacted, so that it is possible to ensure they are being safeguarded. This means a child will have to have access to a ChildLine account- hosted by the NSPCC to create a report. NSPCC are responsible for safeguarding the child, whilst IWF reviews the reported images and videos and reaches a determination on whether or not they are considered illegal. We will always respond to a child and notify them of the outcome of our decision.

We also receive complaints about platforms as part of the Video Sharing Platform regime via Ofcom. More detail about this is [available on their website](#).

19. If you answered 'yes' to question 18, to what extent is information about service users included in those reports?

It depends on the reporting flow and whether a user has requested to receive feedback on their report. If a member of the public has reported to us, they can choose to leave contact details or not.

If a child has reported to us via Report/Remove, we will have an email address through the ChildLine account, so that we can reach the child.

20. If illegal content is detected, is this subsequently reported to another organisation?

Yes

No

Unsure/ not applicable

If yes, what organisation is illegal content reported to and what information about individual service users is included in the reports?

The IWF will report the presence of illegal content on a service directly to the host if the content is hosted in the UK and will do this by issuing a Notice and Takedown (NTD) request. We will also add the image to the Child Abuse Image Database (CAID), the law enforcement database in the UK, so that if the image is found on an offenders device, it can be taken into account at sentencing.

Internationally, we will work through the INHOPE network of hotlines to have content removed. If we have not had a response from an INHOPE hotline within 24 hours of notification, we can then go directly to the host to request removal.

In terms of what is referred to in the reports that we submit, it will be information related to where the offending content is hosted and from that information, it may be possible for a platform or tech company to identify who is responsible for hosting that content.

When notifying the National Crime Agency, it is possible for them to identify victims or offenders through their Victim ID team.

Additional considerations

21. Please describe any further issues (not already covered) that you feel it would be beneficial for the ICO to consider in relation to content moderation.

N/A

22. The ICO is planning to hold further engagement exercises as part of its programme of work on online safety technologies. Would you like to participate in future engagement activities?

Yes

No

If yes, please provide the best contact details:.....

Impacts on your organisation

We would like to understand more about how future ICO guidance and support in this area may impact you or your organisation, and issues that you would find it useful for guidance to cover.

The questions in this section are for developers and/or users of content moderation systems only.

23. Please tell us about the cost implications of content moderation approaches. What aspects of these costs are linked to complying with data protection and privacy law?

This is a question more related to platforms and services than IWF.

24. Please provide information about any other impacts (positive or negative) you are likely to experience from applying data protection and privacy law to your content moderation approaches.

This is a question more applicable to content moderation and platforms.

25. Who in your organisation is likely to use guidance on content moderation? (Please provide job titles or roles, not people's names).

- Hotline Director
- Hotline Manager
- Senior Internet Content Analysts
- Content Analysts
- Quality Assurance Team

All these roles involving ensuring that our data meets UK Sentencing Council Guidelines, and all of our analysts are required to undertake CAID national assessment training.

26. If greater clarity were provided on how the data protection regime and the Privacy and Electronic Communications Regulations (PECR) apply to online content moderation processes, how might that benefit your organisation? Tick all that apply.

- Confidence that you are providing a compliant service / product.
- Marketing / promoting brand
- Increased customer confidence / reassurance
- Increased revenues or profits
- Reduced legal or advisory costs
- Would not benefit
- Other (please specify):

Baseline Monitoring Information

We are interested in current levels of understanding of the UK data protection regime and the Privacy and Electronic Communications Regulations among developers and users of content moderation solutions, and how confident organisations feel in complying with these.

The questions in this section are for developers and/or users of content moderation systems only.

27. Please rate your general understanding of the UK data protection regime (UK General Data Protection Regulation and the Data Protection Act 2018).

- 1 – very low
- 2 – low
- 3 – neither low, nor high
- X 4 – high
- 5 – very high
- Unsure/don't know

28. Please rate your general understanding of the Privacy and Electronic Communications Regulations (PECR).

- 1 – very low
- 2 – low
- 3 – neither low, nor high
- X 4 – high
- 5 – very high
- Unsure/don't know

29. Please rate how confident you are in ensuring the content moderation systems you develop and/or use comply with data protection legislation. Please explain the reasoning for your choice.

- 1 – very low
- 2 – low
- 3 – neither low, nor high
- X 4 – high
- 5 – very high
- Unsure/don't know

Please explain why:

30. Please rate how confident you are in ensuring the content moderation systems you develop and/or deploy comply with PECR legislation. Please explain the reasoning for your choice.

- 1 – very low
- 2 – low
- 3 – neither low, nor high
- X 4 – high
- 5 – very high
- Unsure/don't know

Please explain why: