Date: 19 December 2024

This advice represents the position as at the date the advice provided. Businesses should consult relevant information and guidance on regulators' websites to keep up-to-date with the latest developments.

CASE STUDY:

AI and Online Forums: Navigating Data Protection, Online Safety, and Consumer Law in Health Discussion Forums

This is an anonymised version of a query submitted to the DRCF AI and Digital Hub ('the Hub').

The query in this case study has been responded to by the following DRCF regulators ('we', 'us', 'our'):

- Information Commissioner's Office ('ICO');
- Competition and Markets Authority ('CMA'); and
- Office of Communications ('Ofcom').

This informal advice is provided in line with the Conditions for Participation.

Our informal advice is provided to a business based on our current understanding of the legal and regulatory frameworks within our remits and how they apply to the business's service. This informal advice should not be treated as an exhaustive account of the issues linked to a business's service or represent an endorsement of their proposed innovation.

Our informal advice is specific to a business's circumstances as described by them in the information they provided to the Hub.

Our informal advice is provided without prejudice to any future regulatory intervention by any DRCF or non-DRCF regulator and is not a substitute for independent legal advice which a business may wish to seek in advance of the launch of their service.

It is ultimately a business's responsibility to assess their position under the law and regulatory regime, with the benefit of independent legal advice as necessary. Recognising that some regulatory regimes are still developing and could change over time, businesses have a responsibility to keep up to date with the latest position.

Please note, the queries in this case study appear to engage areas of the law, such as medical regulation and tort law, and raise broader ethical considerations on which the DRCF regulators cannot provide informal advice. Before releasing any service, a business must ensure that they adhere to all applicable laws, guidance, and rules, including by way of example approaches set by other relevant regulators such as the Medicines and Healthcare products Regulatory Agency ('MHRA'). We strongly advise seeking independent legal advice in this regard and encourage businesses to approach relevant authorities and regulatory bodies directly if appropriate. Please note that it is a

business's responsibility to ensure that they identify all such relevant bodies, and seek authorisation, advice and/or guidance from them as applicable. Our informal advice may change if a service evolves or if a business receives specific guidance from other relevant regulatory bodies.

A non-confidential version of the informal advice provided to the applicant is attached to this case study. This informal advice was provided on 19 December 2024 and represents the position as at 19 December 2024. Businesses should consult relevant information and guidance on regulators' websites to keep up to date with the latest developments.

Summary of Query and Response

Business A is a start-up offering a discussion forum where users with specific health issues can find and share their experiences with other individuals. As Business A incorporates AI and third-party data analytics as part of the service, it will need to ensure compliance with relevant regulations.

Business A brought five questions to the DRCF AI and Digital Hub. A summary of the questions and responses is provided below, followed by the full version of the informal advice given to Business A.

Q1: Do we need user consent to share aggregated health information with adtech providers? (p16). The response outlined:

- Explicit user consent is required to share health information with adtech providers. (1.1) Explicit consent requires a higher standard of consent than general consent, as health data is a type of 'special category data'. (1.2)
- The ICO's Opinion on Online Advertising Proposals finds that existing cookie consent mechanisms struggle to meet the higher standard for explicit consent. (1.3)
- As a result, Business A should explore alternative approaches to displaying advertisements to users, such as contextual advertising. (1.4)
- The terms of use for Business A's service should also be fair and transparent, as required by the Consumer Rights Act ('CRA'). This requirement will apply to Business A's user terms generally in addition to their specific application regarding data protection. (1.5)
- A failure by a trader to comply with data protection law may, depending on the circumstances, constitute an unfair commercial practice under the CPRs. (1.6)

Q2: What responsibilities do we have if we use targeted advertisements based on users' health information? (p18). The response outlined:

If Business A proceeds with using targeted advertisements, it should prepare its service by:

- Completing a DPIA to help identify and minimise data protection risks. (2.2)
- Ensuring personal data is "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed", as per data minimisation. (2.3)
- Understanding that processing health data, as a type of special category data, comes with additional responsibilities due to the increased risks involved. (2.4)

When interacting with users Business A:

- Must provide clear and transparent information about its organisation, why it is processing personal data, how the data will be processed and shared, and other relevant information for transparency purposes. (2.5)
- Should ensure the terms of use for its service should also be fair and transparent, as required by the CRA. This requirement will apply to Business A's user terms generally in addition to their specific application regarding data protection. (2.6)
- Should ensure any advertisement Business A publishes is not misleading by act or omission. Business A should ensure that it has appropriate systems and processes in place to prevent and remove false or misleading information in targeted advertising from the forum. (2.7)
- Must recognise that a practice such as targeted advertising can be considered an aggressive practice under the Consumer Protection from Unfair Trading Regulations 2008 ('CPRs') in certain circumstances. (2.8)
- Plan ahead if it intends to send tailored messages to users within the service, this may be considered 'electronic mail marketing'. As such, Business A would need user consent to send those messages or meet the 'soft opt-in' criteria. (2.9)

Q3: What are our obligations in ensuring safe user-to-user interactions? (p23).
The response outlined:

- The Online Safety Act 2023 ('OSA') requires in-scope services to protect people from harm and enable safe U2U interactions. While the OSA has not fully come into force, the first new duties have taken effect with the publication of the Illegal Harms Statement on December 16th, and Business A can start to prepare now.
    - For illegal content, in-scope services must consider carrying out a risk assessment, plan to manage and mitigate risks through the illegal content duties, and prepare to maintain records. The illegal content risk assessment will be the first step. The Risk Assessment Guidance is available on Ofcom's website here, and Business A will need to complete a risk assessment by mid-March 2025. (3.3)
    - For children's safety, in-scope services must consider completing a children's access assessment, carrying out a risk assessment, and preparing for children's safety duties, including around protecting children, content reporting and complaints. The children's access assessment will be the first step. The children's access assessment guidance will be available in January 2025, and Business A should complete an access assessment by mid-April 2025. (3.4)

- Business A should also consider the extent to which consumer laws apply including ensuring that its terms of use are fair and transparent, as required by the CRA. (3.6)
- If users on Business A's forum are business users who are, for example, offering their services to consumer users of the forum, then the CPRs are likely to apply to those businesses. Further, Business A may be required to take steps to tackle unfair commercial practices taking place on or facilitated by the forum to meet its own obligations under consumer law. (3.7)

Q4: What responsibilities do we have if user profiles are set to public by default? (p29). The response outlined:

- Business A should carefully consider to what extent it is necessary to be public by default, especially if children are able to access the service. Business A should consider proceeding with a private by default approach, to ensure a higher level of privacy and protection for its users. (4.1)
- If Business A proceeds with public by default user profiles, it will need to consider:
    - The risks that may arise, particularly relating to illegal content or CHC; (4.3)
    - Being transparent about the collection and use of personal data and how it will be visible to others (under both data protection and consumer protection laws) so that users can take genuine informed choices; (4.4)
    - The requirement that any terms with users about the use of the service are fair and transparent as required by the CRA; (4.5)
    - Including an easy and straightforward mechanism which allows users to switch to private by default; (4.6)
    - Implementing effective content moderation to prevent users from encountering illegal content or CHC; (4.7)
    - Effective reporting and complaints for users to report illegal content or CHC; (4.8) and
    - Implementing highly effective age assurance to prevent children from encountering primary priority content and protecting them from priority content. (4.9)
- If Business A maintains user profiles as public by default, children will be at heightened risk. For children, settings must be high privacy by default. (4.10)

Q5: What responsibilities do we have if we use AI to make health recommendations as "best suggestions" to users? (p33). The response outlined:

- Please note, Business A's queries appear to engage areas of the law, such as medical regulation and tort law, and raise broader ethical considerations that the DRCF regulators cannot provide informal advice on. Before releasing any service, businesses must ensure that it adheres to all applicable laws, guidance and rules, including by way of example approaches set by other relevant regulators such as the Medicines and Healthcare products Regulatory Agency ('MHRA'
- Using AI to make health recommendations, including under the term "best suggestions" or similar, requires careful attention of the consumer protection, data protection, and online safety implications.
- Business A should particularly note banned practice 17 of the CPRs which prohibits falsely claiming that a product is able to cure illnesses, dysfunction or malformations. (5.1)
- Business A should review the CMA's AI Foundation Models Initial Review which identifies potential consumer protection concerns related to foundation models. (5.2)
- If Business A has considered its legal obligations and established that it will not infringe the CPRs by making health recommendations as "best suggestions" in these circumstances, it will need to produce a DPIA (5.3) and conduct risk assessments (5.4) to identify and mitigate data protection and online safety risks.
- When providing "best suggestion" to users:
    - Business A must ensure that the information it provides to users via health recommendations is not misleading. (5.5) It should consider and follow the recommendations set out in CMA guidance on the Trader Recommendation Platforms as it relates to user reviews to reduce the risk of infringing consumer law. (5.6)
    - Business A should document in its DPIA how it will maintain statistical accuracy of its recommendations and what steps it will take to moderate potentially harmful content. (5.7)
    - Business A should also not omit or hide 'material information' from its "best suggestions". (5.8)
    - Business A should consider the requirement that any terms with users about the use of its service are fair and transparent as required by the CRA. (5.9)
    - Business A should note that data protection law applies to all automated individual decision-making and profiling. (5.10)

- In addition to the below response, Business A should apply the advice provided in:
    - **Question 2,** for data protection guidance on special category data, purpose limitation, data minimisation, transparency and individual rights, to this processing activity.
    - **Question 3,** for online safety guidance specific to illegal harms and protection of children.

Date: 19 December 2024

This advice represents the position as at the date the advice provided. Businesses should consult relevant information and guidance on regulators' websites to keep up-to-date with the latest developments.

Table of Contents

Queries submitted to the Hub

Business A is a start-up offering a discussion forum where users with specific health issues can find and share their experiences with other individuals. As Business A incorporates AI and third-party data analytics as part of the service, it will need to ensure compliance with relevant regulations. Business A's questions are:

- Do we need user consent to share aggregated health information with adtech providers? (p16)
- What responsibilities do we have if we use targeted advertisements based on users' health information? (p18)
- What are our obligations in ensuring safe user-to-user interactions? (p23)
- What responsibilities do we have if user profiles are set to public by default? (p29)
- What responsibilities do we have if we use AI to make health recommendations as "best suggestions" to users? (p33)

Introduction to the ICO, CMA and Ofcom

Business A's queries have been responded to by the ICO, CMA and Ofcom. A brief introduction to each regulator has been included below.

Each regulator is responsible for separate legal regimes with different requirements that may be applicable to the same set of facts, and it will be necessary to take steps to comply with each regime as set out.

ICO

The Information Commissioner's Office ('ICO') is the UK's independent public authority set up to uphold information rights. The ICO oversees the following data protection and privacy laws which are relevant to this informal advice:

- the UK General Data Protection Regulation ('UK GDPR');
- the Data Protection Act 2018 ('DPA 2018'); and
- the Privacy and Electronic Communications Regulations 2003 ('PECR').

Under the **UK GDPR** and **DPA 2018**, organisations must consider data protection and privacy issues upfront in everything they do. Organisations must bake in privacy considerations from the design stage throughout the product development lifecycle.

The UK GDPR sets out seven key principles:

- lawfulness, fairness, transparency;
- purpose limitation;
- data minimisation;
- accuracy;
- storage limitation;
- integrity and confidentiality (security); and
- accountability.

These principles lie at the heart of UK GDPR, informing everything that follows, and are key to organisations' compliance with law. The informal advice that follows highlights some of these considerations for Business A's intended processing activities.

The UK GDPR also gives everyone rights over how their personal information is used. These individual rights include a right to:

- be informed;
- access and receive a copy of their personal data;
- have inaccurate data rectified;

- not be subject to automated decision-making and profiling; and
- have personal data erased.

Organisations must ensure people can exercise these rights.

PECR sits alongside the UK GDPR. They give people specific privacy rights in relation to electronic communications which are relevant for Business A's service, including on:

- marketing calls, emails, texts and faxes; and
- cookies (and similar technologies).

CMA

The Competition and Markets Authority ('CMA') is the UK's lead competition and consumer authority and an independent non-ministerial department of the UK government. The CMA helps people, businesses and the UK economy by promoting competitive markets and tackling unfair behaviour. The CMA's ambition is to promote an environment where consumers can be confident that they are getting great choices and fair deals, and competitive, fair-dealing businesses can innovate and thrive. The CMA enforces the following laws which are relevant to this informal advice:

- the Consumer Protection from Unfair Trading Regulations 2008 ('CPRs'); and
- the Consumer Rights Act 2015 ('CRA').

The **CPRs** prohibit unfair commercial practices which may harm consumers' economic interests. Broadly speaking, the CPRs prevent 'traders' from treating consumers unfairly. Trader means a person acting for purposes relating to their business whether acting personally or through another person acting in their name or on their behalf. The CPRs will apply to a trader's commercial practice if it is directly connected with the promotion, sale or supply of goods or services to (or from) consumers. As such, the CPRs apply to a wide range of commercial activities involving consumers such as advertising, marketing, sales, supplies and after-sales services.

In the CMA's responses to Business A's questions, the CMA considers that Business A is likely to be a trader for the purpose of the CPRs. The CMA sets out some key information on the CPRs here, which apply to each of Business A's questions. The CPRs prohibit:

- Commercial practices that contravene the requirements of professional diligence (meaning honest market practice and good faith in Business A's field of activity) and which materially distort or are likely to materially distort the economic behaviour of the average consumer.
- Misleading actions, which occur when i) a trader gives consumers false information (about a wide range of things listed in the CPRs) or where the trader's practice or its overall presentation in any way deceives or is likely to deceive the average consumer (even if the information is factually correct), and ii) the

practice causes or is likely to cause the average consumer to take a different decision.

- Misleading omissions, which occur when a trader fails to give consumers the information that they need, according to the context, to take an informed decision and the average consumer takes, or is likely to take, a different decision as a result. This includes a) omitting or hiding this 'material information', b) providing it in an unclear, unintelligible, ambiguous or untimely manner, or c) if the commercial practice fails to identify its commercial intent (unless already apparent from the context).

The CPRs look at the effect of a commercial practice on the notional 'average consumer' whom the practice reaches or is addressed to, and who is taken to be reasonably well informed and reasonably observant and circumspect. Where a commercial practice is directed at a particular group of consumers or where a clearly identifiable group is particularly vulnerable to the practice in a way the trader could reasonably be expected to foresee – e.g. because of their mental or physical infirmity – Business A commercial practice will be assessed by reference to the average member of that group. Since Business A is offering a discussion forum where users with health conditions find and share their experiences with other individuals, those individuals are likely to be considered vulnerable consumers and the notional average consumer will be considered to be the average member of that group.

The CPRs will be repealed and replaced by the **Digital Markets, Competition and Consumers Act 2024 ('DMCCA')**, when the relevant part of the legislation comes in force in 2025. However, the informal advice referred to in this response is likely to be substantially unchanged in practice.

The **CRA** requires that terms in consumer contracts and notices must be fair. Written terms need to be transparent, which means written in a way that is clear and legible, uses plain language, and that enables consumers to properly understand the consequences of a term. Under the CRA, traders which contract with UK consumers to supply digital content must also ensure it is of satisfactory quality, fit for purpose and as described.

In the context of this informal advice, the CMA will refer to 'consumers' on Business A's forum as 'users', unless stated otherwise.

It should be noted that although guidance from the CMA is concerned with the application of consumer law in these circumstances, failing to comply with other sector-specific and general laws, such as medical regulations, standards and guidelines, is a matter that the CMA would take account of when assessing whether consumer law has been infringed.

The examples given in the CMA's response below are for indicative purposes, and whether a particular practice breaches the CPRs will require a case-by-case

assessment based on the particular facts and circumstances. In its response, the CMA does not set out every situation or practice in which a breach of the CPRs may occur. This informal advice is not a substitute for legal advice and should not be relied on as such.

Consumer protection interactions with data protection in relation to Business A's questions

The processing of personal data is primarily regulated by the UK GDPR. However, a failure by a trader to comply with data protection law may, depending on the circumstances, constitute an unfair commercial practice under the CPRs.

The CPRs apply not just to "paid for" services (i.e. where consumers pay money to use them) but also apply to 'free' products where services are provided in exchange for consumers' personal data (as personal data has economic value).

A trader's failure to comply with the UK GDPR could, depending on the circumstances, contravene the requirements of professional diligence under the CPRs or constitute a misleading commercial practice. In these circumstances, a failure by Business A to be transparent about the collection of consumers' personal data and the fact that it may be used for commercial purposes, or otherwise failing to give consumers a genuine informed choice about how their data will be used, may constitute a breach of the CPRs.

Although an infringement of data protection law will not automatically constitute a breach of consumer law, the CMA is likely to take this into account when assessing the overall unfairness of a trader's commercial practice under the CPRs.

In addition, under the CRA, any contract wording which could have the effect of depriving consumers of protection normally afforded to them under the law is liable to be considered unfair. For example, a term or statement which could be understood as permitting a trader to deal more freely with a consumer's personal data (particularly sensitive personal data) than the law allows – for example, to pass it on more widely – is likely to be open to challenge as unfair.

This summary is in particular relevant for questions 1, 2 and 4.

Ofcom

Ofcom is the regulator for the communications services that people and businesses use and rely on each day. Ofcom regulates the TV and radio sectors, fixed line telecoms, mobile, postal services, plus the airwaves over which wireless devices operate. In addition, Ofcom has been appointed as the regulator for online safety. Ofcom oversees the following laws which are relevant to this informal advice:

- Online Safety Act 2023 ('OSA').

Under the **OSA**, Ofcom's mission is to make life safer online in the UK, especially for children, by ensuring services have the appropriate systems and processes to protect people from harm. While the OSA has not fully come into force yet, the first new duties have taken effect with the publication of the Illegal Harms Statement on December 16th, and Business A can start to prepare now.

For a comprehensive overview of the OSA and Ofcom's roadmap to regulation, please see here.

Online services need to determine whether they are in scope of the Online Safety Act, and bring themselves into compliance if they are. Under the OSA there are three categories of services that will be legally responsible for keeping people, especially children, safe online. This includes:

- **User-to-user (U2U) services,** where people can create and share content (e.g. images, videos, messages or comments), or interact with each other;
- **Search services,** where people can search more than one website and/or database; and
- **Pornography services,** where an individual or a business publishes or displays pornographic content.

Based on Ofcom's understanding of Business A, its product may be considered a U2U service under the OSA because:

- the service enables users to interact with one another, including by generating, uploading or sharing content, such as images, videos, messages or comments, with other users of the service; and
- the service intends to have links with the UK:
    - by having either a significant number of UK users or the UK being a target market for the service as per section 4(5) of the OSA; or
    - by being capable of being used in the United Kingdom by individuals, and there are reasonable grounds to believe that there is a material risk of significant harm to individuals in the United Kingdom presented by user-generated content present on the service as per section 4(6) of the OSA.

As a result, for the purpose of the informal advice, Ofcom has treated Business A as a U2U service. Depending on the product launch and development, Business A should also consider whether its product may be considered as a search service or a combined service.[1]

[1] Under Section 4(7) of the OSA a combined service refers to a regulated U2U service that includes a public search engine as well.

Regulator Response References

The table below indicates which regulator has provided the informal advice in each paragraph. Ofcom, the CMA and ICO are separate regulatory bodies and they are only responsible for the parts of this informal advice which they have contributed, as set out in the table below.

Regulator	Question	Relevant Responses
ICO	Q1	1.1 - 1.4
	Q2	2.2 - 2.5, 2.9
	Q3	
	Q4	4.1, 4.4, 4.6, 4.10
	Q5	5.3, 5.7, 5.10
CMA	Q1	1.5, 1.6
	Q2	2.1, 2.6 -2.8
	Q3	3.6 - 3.7
	Q4	4.5, 4.6
	Q5	5.1, 5.2, 5.5, 5.6, 5.8, 5.9
Ofcom	Q1	
	Q2	
	Q3	3.1 - 3.5
	Q4	4.3, 4.7, 4.8, 4.9
	Q5	5.4

Response

1. Do we need user consent to share aggregated health information with adtech providers?

Summary

- Explicit user consent is required to share health information with adtech providers. (1.1) Explicit consent requires a higher standard of consent than general consent, as health data is a type of 'special category data'. (1.2)
- The ICO's Opinion on Online Advertising Proposals finds that existing cookie consent mechanisms struggle to meet the higher standard for explicit consent. (1.3)
- As a result, Business A should explore alternative approaches to displaying advertisements to users, such as contextual advertising. (1.4)
- The terms of use for Business A's service should also be fair and transparent, as required by the CRA. This requirement will apply to its user terms generally in addition to their specific application regarding data protection. (1.5)
- Business A should also see the section above about the interaction between data protection and consumer protection law and make sure that its practices comply with consumer protection law. (1.6)

Response

1.1. Yes, explicit user consent is required to share health information with adtech providers. If Business A plans to use Cookies or Similar Technologies to collect and share health data, it must comply with both the **Privacy and Electronic Communications Regulations ('PECR')** and the **UK General Data Protection Regulation ('UK GDPR')**. Specifically:

- **PECR:** Consent is required to set online advertising cookies on a user's device.
- **UK GDPR:** Consequently, the lawful basis under the UK GDPR for setting cookies that collect personal data must also be consent.

1.2. Health data, as a type of 'Special Category Data' under the UK GDPR, requires additional protection due to its sensitive nature. To process health data, Business A must meet one of the conditions outlined in Article 9 of the UK GDPR, which sets out the requirements for processing special category data. The only valid Article 9 condition for processing user's health information for online advertising purposes is explicit consent. This means that explicit consent will be required for the initial

collection of health information through cookies and any subsequent sharing of that information with adtech providers.

Explicit consent *requires a higher standard of consent than general consent, meaning the user must make an express statement agreeing to the use of their health data for advertising. More guidance on obtaining Explicit Consent can be found within the link provided.*

1.3. Business A should note that the ICO Opinion on Online Advertising Proposals (page 17) found that existing cookie consent mechanisms struggle to meet the higher standard for explicit consent, which could make compliance challenging.

1.4. In light of this, the ICO recommends exploring alternative approaches to displaying advertisements to users. Some of these approaches are outlined in the opinion, such as contextual advertising. Contextual advertising places advertisements based on the content of a webpage rather than tracking user behaviour. This approach is more privacy-friendly, and would not require Business A to use cookies to collect user health data or share this information with third parties.

1.5. The CRA requires that terms in consumer contracts and notices must be fair. Written terms need to be transparent, which means written in a way that uses plain language, and that enables consumers to properly understand the consequences of a term. This applies to Business A's user terms generally in addition to their specific application regarding data protection. Business A should consider referring to the CMA's Unfair contract terms guidance: CMA37 which sets out the CMA's understanding of the provisions in the CRA which deal with unfair contract terms and notices.

1.6. Business A should also see the section in the introduction to the CMA about the interaction between data protection and consumer protection law and make sure that its practices comply with these consumer protection rules.

2. What responsibilities do we have if we use targeted advertisements based on users' health information?

Summary

If Business A proceeds with using targeted advertisements, it should prepare its service by:

- Completing a DPIA to help identify and minimise data protection risks. (2.2)
- Ensuring personal data is "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed", as per data minimisation. (2.3)
- Understanding that processing health data, as a type of special category data, comes with additional responsibilities due to the increased risks involved. (2.4)

When interacting with users Business A:

- Must provide clear and transparent information about its organisation, why it is processing personal data, how the data will be processed and shared, and other relevant information for transparency purposes. (2.5)
- Should ensure the terms of use for its service should also be fair and transparent, as required by the CRA. This requirement will apply to Business A's user terms generally in addition to their specific application regarding data protection. (2.6)
- Should ensure any advertisement Business A publishes is not misleading by act or omission. Business A should ensure that it has appropriate systems and processes in place to prevent and remove false or misleading information from the forum. (2.7)
- Must recognise that a practice such as targeted advertising can be considered an aggressive practice under the CPRs in certain circumstances. (2.8)
- Plan ahead if it intends to send tailored messages to users within the forum, this may be considered 'electronic mail marketing'. As such, Business A would need user consent to send those messages or meet the 'soft opt-in' criteria. (2.9)

Response

2.1. If Business A plans to use targeted advertisements based on users' health information, it needs to consider several key responsibilities under data protection (**UK GDPR)** and **consumer protection (CRA and CPRs) laws**. These considerations are not exhaustive but are a useful starting point:

Preparing the service

2.2. **Data Protection Impact Assessment ('DPIA'):** DPIAs are tools that organisations can use to identify and minimise the data protection risks of any processing. Article 35 of the UK GDPR specifies several circumstances that require DPIAs, including where there is large-scale processing of special category data, like health data.

Given the risks associated with targeted advertisements based on health data, such as the potential for invisible processing or unwanted profiling, Business A must complete a DPIA before beginning any processing. The DPIA will help Business A identify and mitigate risks, such as obtaining explicit consent.

2.3. **Data Minimisation:** Under the UK GDPR, personal data must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed." This means Business A must ensure it only processes the minimum amount of personal data needed for online advertising.

Contextual advertising, as outlined in Question 1, aligns more easily with the data protection principles, especially data minimisation, as it often does not require the processing of personal data. The ICO recommends assessing whether the intended outcomes can be achieved without using personal data, particularly special category data.

If Business A determines that processing personal data, including health data, is necessary, it must document its rationale in its DPIA, and for the purpose of data minimisation, outline the steps taken to reduce the amount of personal data processed.

2.4. **Special Category Data:** Processing special category data comes with additional responsibilities due to the increased risks involved. This includes maintaining detailed records that clearly document the categories of personal data Business A holds on its users. In addition, Business A must implement strong security measures to protect special category data. These are just a couple of examples of the additional responsibilities associated with processing special category data. The ICO recommends reviewing the link provided for further guidance.

Interacting with users

2.5. **Transparency:** Transparency is a fundamental principle within UK GDPR. It ensures that users understand how their personal data is used and enables them to exercise their data protection rights. As noted above, this is particularly important in the context of online advertising where the reasons for seeing certain advertisements may not always be clear to users.

To meet its transparency obligations under data protection, Business A should provide clear and comprehensive information. This includes:

- The organisation's name and contact details.
- The purposes for processing personal data.
- The lawful basis for processing personal data and special category data.
- How the data is collected.
- Who the data is shared with.
- Information on users' data protection rights, including their right to withdraw consent.

Individuals also have specific data protection rights that are particularly relevant for targeted advertisements. Two examples of these are:

- The right of access (e.g. if a user requests details about who a business has shared their health data with for targeted advertisements).
- The right to object (e.g. if a user asks a business to stop processing their health data for targeted advertisements).

Business A should familiarise itself with all Individual Rights and ensure it has robust processes in place to handle them effectively.

2.6. **Fair and Transparent terms:** Business A should also ensure that the terms of use for its service, as provided to users, are fair and transparent, as required by the CRA. This applies to Business A's user terms generally in addition to their specific application regarding data protection, as explained above. The CMA refers Business A again to the CMA's Unfair contract terms guidance: CMA37.

2.7. **Misleading Practices:** As set out in the introduction to consumer protection law, Business A should ensure that it does not engage in misleading actions or omissions under the CPRs.

- In addition to the transparency principle for data protection, under the CPRs, Business A must provide users with the information they need to take an informed decision about using the service. In particular, Business A's users are likely to need to know that their information is collected and used for targeted advertising so that they can decide whether they want to accept this. Business A should also see the section in the introduction to the CMA '*Consumer protection interactions with data protection in relation to Business A's questions',* in particular, in relation to the CPRs – and make sure that its practices comply with these consumer protection rules.
- Further, Business A must not publish misleading advertisements (whether they are misleading by action or omission). An advertisement is likely to comprise or result in a misleading action if it gives users false information or if its overall presentation in any way deceives, or is likely to deceive, the

'average consumer' (about a wide range of things listed in the CPRs, including the nature of the product, its main characteristics, and the consumer's rights or the risks they may face), and this causes or is likely to cause the 'average consumer' to take a different decision as a result. The notional 'average consumer' is taken to be reasonably well informed and reasonably observant and circumspect, as explained in the 'Introduction to the CMA', above. Further, where advertising is targeted at a particular group of consumers or where a clearly identifiable group is particularly vulnerable to the practice in a way that Business A could reasonably be expected to foresee – which is likely to be the case here based on Business A's description of its users, the notional 'average consumer' will be the average member of that group. Advertisements are likely to be misleading by omission if they fail to give consumers the information that they need to make an informed choice in relation to a product (including where such 'material information' is omitted, hidden or provided in an unclear, unintelligible, ambiguous or untimely manner), and the average consumer takes, or is likely to take, a different decision as a result. See the unfair commercial practices guidance for more information. Note that the CMA will soon be consulting on updated unfair trading guidance under the DMCCA and the CMA recommends Business A keeps itself updated.

- **Appropriate systems and processes:** To reduce the risk of infringing the CPRs, Business Ashould ensure that it has appropriate systems and processes in place to prevent and remove false or misleading information from publication. If Business A does not have the appropriate systems and processes in place, it may also contravene the requirements of professional diligence and infringe the CPRs where this materially distorts the 'average consumer's' economic behaviour – for example where they take a decision to buy an advertised product.

2.8. **Aggressive Practices:** If a commercial practice significantly impairs, or is likely to significantly impair, the "average consumer's" freedom of choice through the use of harassment, coercion or undue influence and that then impacts their decisions, that will be a prohibited aggressive practice and under the CPRs. In deciding whether a commercial practice is aggressive, account is taken of a list of factors specified in the CPRs which include, for example, the exploitation of any specific misfortune or circumstance of such gravity as to impair the consumer's judgement. Business A should bear these obligations in mind when considering how targeted advertising is presented to users on its forum and, for example, whether the online choice architecture may put pressure on them to purchase particular products or take a certain action which could subsequently lead to a

purchase. Again, see unfair commercial practices guidance and updated DMCCA guidance for more information.

2.9. **Electronic Mail Marketing:** If Business A plans to send users tailored messages based on their interaction with its service, this may be considered 'electronic mail marketing' under PECR. In such cases, Business A must ensure that it has the user's consent for this, or meet the criteria for the 'soft opt-in' exception. To meet 'soft opt-in', Business A would need to satisfy three criteria:

- Business AObtained the user's contact details during a sale, or the negotiations for a sale, for the service.
- The messages it sends relate to similar products or services (e.g. posts or promotional material the user has already shown interest in).
- Provide the user with a simple opt-out opportunity at the time their contact details were collected and further opt-out opportunities are provided.

3. What are our obligations in ensuring safe user-to-user interactions?

Summary

- The Online Safety Act 2023 ('OSA') requires in-scope services to protect people from harm and enable safe U2U interactions. While the OSA has not fully come into force, the first new duties have taken effect with the publication of the Illegal Harms Statement on December 16th, and Business A can start to prepare now.
    - For illegal content, in-scope services must carry out a risk assessment, plan to manage and mitigate risks through the illegal content duties, and prepare to maintain records. The illegal content risk assessment will be the first step. The Risk Assessment Guidance is available on Ofcom's website here, and Business A will need to complete a risk assessment by mid-March 2025. (3.3)
    - For children's safety, in-scope services must complete a children's access assessment, and prepare to carry out a risk assessment, and prepare for the children's safety duties, including around protecting children, content reporting and complaints. The children's access assessment will be the first step. The children's access assessment guidance will be available in January 2025, and Business A should complete an access assessment by mid-April 2025. (3.4)
- Business A should also consider the extent to which consumer laws apply including ensuring that its terms of use are fair and transparent, as required by the CRA. (3.6)
- If users on Business A's forum are business users who are, for example, offering their services to consumer users of Business A's forum, then the CPRs are likely to apply to those businesses. Further, Business Amay be required to take steps to tackle unfair commercial practices taking place on or facilitated by the forum to meet its own obligations under consumer law. (3.7)

Response

3.1. As noted in the introduction, for the purpose of this informal advice Ofcom will treat Business A as a U2U service regulated under the OSA. However, Business A should also assess whether its forum might be classified as a 'search service'. Ofcom recommends using Ofcom's dedicated Online Safety Regulation Checker tool, which can help businesses determine whether their services fall under the classification of a 'search service' in addition to being a U2U service.

3.2. During 2025, the OSA will start to require U2U services to protect people from harm and enable safe U2U interactions through, at a minimum, the **Illegal Content and Children's Safety Duties.** Further details are outlined below.

3.3. **Illegal Content Duties:** Ofcom has published its Illegal Harms Statement which sets out the obligations that providers of U2U services have in respect to illegal content and enabling safe U2U interactions. Please refer to the timeline here and below for relevant timelines related to this section:

- **16 December 2024:** Ofcom published the Illegal Harms Statement. This includes the first edition of the Illegal Content Codes, and Risk Assessment Guidance for Service Providers. These Codes will be submitted to the Secretary of State for approval.
- **December 2024 – March 2025:** Services complete illegal content risk assessments.
- **March 2025:** The Illegal Content Codes come into force following the completion of the Parliamentary process to approve them. Providers of in-scope services must comply with the relevant safety duties and Ofcom can enforce against non-compliance.

Specific informal advice for Business A is included below:

- **Illegal content risk assessment:** Ofcom published the Illegal Harms Statement which includes illegal content Risk Assessment Guidance, available here. The risk assessment is the first step for Business A to assess the risk of harm to users arising from illegal content on the forum, to understand what safety measures Business A needs to put in place to protect users. Ofcom has created the Risk Assessment Guidance for Service Providers to help Business A complete an illegal content risk assessment and meet its duties under the OSA. Business A will find it useful to review this guidance to help it complete its assessment. Whether or not Business A follows the guidance, Business A must consult Ofcom's risk profiles as part of its risk assessment. These are designed to help businesses identify relevant risk factors for each kind of illegal content they need to assess.
- **Managing and mitigating illegal harms:** After conducting a risk assessment, Business A should work to manage and mitigate the risk of harm from illegal content on its service, in accordance with relevant safety duties. Providers must comply with the safety duties covered in the Statement from **mid-March 2025.** They include:
    - A duty to take or use proportionate measures relating to the design or operation of the service to **prevent individuals from encountering priority illegal content and minimising the length of time that such content is present on the service**; and

- A duty to operate the service using proportionate systems and processes designed to **swiftly take down any illegal content** when they become aware of it (the 'takedown duty').

The safety duties also require providers of services to include provisions in their terms of service specifying how individuals are to be protected from illegal content, and to apply these provisions consistently. These duties have been broken down by each type of offence for U2U services here.

- **Record-keeping and review:** In addition to the above duties, Business A should ensure records are being kept of decisions about user safety, under the record-keeping and review duties. Providers must comply with the illegal content record-keeping duties from **mid-March 2025.** These duties require providers to:
  - Keep written records of their risk assessments;
  - Keep written records of measures taken as described in a Codes to comply with a relevant duty; and
  - Where the measure described in a Codes has not been taken, keep a written record of the alternative measure taken and how that fulfils the relevant duty.

  To comply with the record-keeping duties, Business A should make and keep written records that are durable, accessible, easy to understand, and up to date. Business A should retain a user's records for at least three years. Ofcom's Record Keeping and Review Guidance provides more information on what the record of risk assessments and the record of Codes or alternative measures should include.

  Business A must review its compliance with each of the online safety duties regularly and update its records with a frequency that allows for a continuous cycle of implementation, monitoring, and review. Ofcom expects providers to undertake a compliance review at least once a year as a minimum. Business A must also review its compliance as soon as possible after making any significant change to the design or operation of the service.
- The Illegal Harms Statement includes a range of important additional guidance to providers, including Ofcom's Illegal Content Judgements Guidance (which helps providers determine whether a piece of content is illegal or not), Enforcement Guidance (setting out Ofcom's approach to enforcement for Online services) and Ofcom's Public Private guidance (which sets out how providers can consider whether a piece of content is communicated publicly).

3.4. **Children's Safety Duties:** Securing a higher level of protection online for children is one of the objectives of the OSA. The OSA places duties on services that will likely be accessed by children, with particular attention to "content that is harmful to children" (CHC). The below information is based on draft guidance, and businesses can refer to the timeline here and below for expected final timelines:

- **January 2025:** Ofcom finalises Children's Access Assessment Guidance.
- **January – April 2025:** Services will have 3 months to complete their children's access assessments.
- **April 2025:** Ofcom expects to publish the Protection of Children Statement, which will include the Protection of Children Codes. These Codes will be submitted to the Secretary of State for approval. Alongside the statement, Ofcom will publish the final Children's Risk Assessment Guidance.
- **April – July 2025:** Services will have 3 months to complete their children's risk assessments.
- **July 2025:** Protection of Children Codes come into force following the completion of the Parliamentary process to approve them. Services must comply with the children safety duties and Ofcom can enforce against non-compliance.

A summary of Ofcom's protection of children proposals is available here and specific informal advice for Business A is included below.

- **Children's Access Assessment:** Business A must complete a **children's access assessment** to establish whether its service is likely to be accessed by children. The final Children's Access Assessment Guidance will be published in **January 2025** and Business A will need to complete its assessment by April 2025. It will help to evaluate:
    - **Stage 1:** Is it possible for children to normally access the services? Please note that Ofcom expects that this condition will be met unless services are using highly effective age assurance ('HEAA').
    - **Stage 2:** Are there any significant numbers of children who are users of the service? Is this service of a kind likely to attract a significant number of children? If the answer to both of those questions is no, then Business A can conclude the children user condition is not met. If the answer to either of these questions is yes, then the service is 'likely to be accessed by children'. Ofcom expects that most U2U services will be 'likely to be accessed by children'. Please refer to Ofcom's quick guide to children's access assessments for more information.

- **Children's Risk Assessment**: If Business A's children's access assessment identifies that children are likely to access the service, it must complete a **children's risk assessment**. The children's risk assessment helps services to identify risks to children and implement effective safety measures to mitigate those risks. The Children's Risk Assessment Guidance will be published in **April 2025** and will need to be completed by July 2025.
    - Children's risk assessments must be suitable and sufficient, meaning it should reflect risks accurately based on the timing of Business A's assessment cycle. Whether or not Business A follows the guidance, it must consult Ofcom's risk profiles as part of its risk assessment. These are designed to help businesses identify relevant risk factors for each kind of CHC they need to assess.
- **Managing and Mitigating CHC:** Business A must follow several duties to protect children online, as outlined Ofcom's consultation, including:
    - The **safety duties protecting children** (section 12);
    - So far as it relates to the protection of children, the **duty about content reporting** (section 20); and
    - So far as it relates to the complaints set out in section 21(5), the **duties about complaints procedures** (section 21).

  The Codes set out measures which services can adopt to help them to comply with the duties in the OSA. A summary of the proposed recommended measures has been included in the Protecting Children: Proposed Codes at a Glance. These are only proposed recommended measures. Services can choose other measures, so long as they remain compliant with their duties. Business A should also refer to the Guidance on Content Harmful to Children to help determine whether content on its service amounts to CHC content. Examples of both what Ofcom considers to be, and considers not to be, each kind of content harmful to children are provided, as well as contextual factors to consider when determining the nature of content.

3.5. The above provides an overview of the key duties and actions required to ensure safe U2U interactions under the OSA. Ofcom recognises that in-scope services are very different, in their size, resources and the risks they pose to people in the UK. Different safety measures will be appropriate for different types of services and Ofcom's recommendations will vary for services depending on their size and degree of risk.

Beyond Ofcom's OSA, Business A should also consider the extent to which consumer protection applies. For example:

3.6. **Fair and Transparent Terms**: As with other responses, Business A should also ensure that its terms with users are fair and transparent, as required by the CRA. Business A should note that it cannot use consumer terms or notices to restrict liability for death or personal injury resulting from its negligence. The CMA refers Business Ato its Unfair contract terms guidance: CMA37 for further information.

3.7. **Business Users**: If users on Business A's forum are business users who engage with consumers in relation to the promotion, sale or supply of products – for example, where they offer or promote their professional services to consumer users of its forum – then the CPRs will apply to those businesses.

- Where Business A's forum allows businesses to interact with consumer users, any representations it makes about its service and the business users on the forum should be clear and accurate, and must not mislead consumer users – for example, where the forum is a trader recommendation platform (as defined by the CMA). The representations may, depending on the circumstances, be about Business A's consumer-facing service or the quality, reliability or suitability of businesses that appear on its forum or the steps it takes to ensure the quality of those businesses as required by consumer law – see improving trader recommendation platforms: consumer law compliance advice for businesses.
- Further, where businesses engage with consumers through Business A's forum, they may contravene the requirements of professional diligence and infringe the CPRs where they do not take such appropriate steps as are necessary to prevent and remove false or misleading information, or otherwise tackle other unfair commercial practices, from third parties e.g. identifying and removing content posted by business users which infringes consumer law. Business A is ultimately responsible for the content it publishes or otherwise makes available to consumers via the forum, and consumer users should be able to trust the information that is presented to them.

Business A will find more information on their responsibilities regarding third parties in the CMA's response to Question 5.

4. What responsibilities do we have if user profiles are set to public by default?

Summary

- Business A should carefully consider to what extent it is necessary to be public by default, especially if children are able to access the service. Business A should consider proceeding with a private by default approach, to ensure a higher level of privacy and protection for its users. (4.1)
- If Business A proceeds with public by default user profiles, it will need to consider:
    - The risks that may arise, particularly relating to illegal content or CHC; (4.3)
    - Being transparent about the collection and use of personal data and how it will be visible to others (under both data protection and consumer protection laws) so that users can take genuine informed choices; (4.4)
    - The requirement that any terms with users about the use of Business A's service are fair and transparent as required by the CRA; (4.5)
    - Including an easy and straightforward mechanism which allows users to switch to private by default; (4.6)
    - Implementing effective content moderation to prevent users from encountering illegal content or CHC; (4.7)
    - Effective reporting and complaints for users to report illegal content or CHC; (4.8) and
    - Implementing highly effective age assurance to prevent children from encountering primary priority content and protecting them from priority content. (4.9)
- If Business A maintains user profiles as public by default, children will be at heightened risk. For children, settings must be high privacy by default. (4.10)

Response

4.1. When a user's profile is set to public by default, it typically means that certain elements of their profile, such as their username, personal information (e.g. name, gender, pronouns), interests, or content they create (which may include identifiable information like images or personal opinions), are accessible to others. This can raise concerns about how much personal data is being shared, the potential for data misuse, and risk harmful content being shared, especially if users are unaware of the default settings or the extent of the information being

shared. Business A should carefully consider to what extent it is necessary, and whether users expect, to have certain types of information included in these public profiles by default.

4.2. Informal advice is provided below. Business A should consider its responsibilities and the potential implications if it chooses to maintain user profiles as public by default.

Preparing the service

4.3. **Identifying and Mitigating Harm with Risk Profiles:** A good starting point to consider whether to set user profiles as public by default is to consider the harms that may occur on the forum. Ofcom has developed **risk profiles** to help services understand the type of harms that are most likely to occur on their service. Details on the risk profiles are available in:

- Protecting People from Illegal Harm Online - Risk Assessment Guidance and Risk Profiles
- Children's Draft Risk Assessment Guidance, Annex 1

As outlined in the documents, certain risks are associated with specific types of illegal harms and CHC. Where relevant Business A must protect against these harms by undertaking risk assessments and complying with the applicable safety duties to ensure users are safe online. There is a heightened risk for children as they may be exposed to a range of CHC. As a result, if Business A's service is 'likely to be accessed by children' having completed a children's access assessment, it must complete a children's risk assessment and comply with the Protection of Children Codes, as outlined in response to Question 3.

Services must complete the illegal content risk assessment between **December 2024 – March 2025** and the children's risk assessment between **April – July 2025**.

Hosting "public by default" users

4.4. **Transparency:** Businesses must be transparent with users from the outset about what personal data will be visible to others and why a public by default approach is necessary. This information should be clear and easily accessible in a privacy notice and during the sign-up process.

4.5. **Fair and Transparent Terms:** Business A should ensure that any terms with users about the use of its service are fair. Written terms need to be transparent, which means written in a way that uses plain language, and that enables consumers to properly understand the consequences of a term. The requirement applies to the user terms generally in addition to their specific application regarding data protection.

Business A should also see the section in the introduction about the interaction between data protection and consumer protection law and make sure that its practices comply with these consumer protection rules.

4.6. **User Control:** Users should have an easy and straightforward way to switch their profile to private if they wish. As the ICO-CMA's Joint Paper on Harmful Designs states, Business A should not use language that may discourage users or penalise them for choosing a private setting. Clear instructions should be provided on how to adjust these settings, and there should be no unnecessary barriers to changing them.

4.7. **Content Moderation:** Effective content moderation will be necessary to prevent users, especially children, from encountering illegal content or CHC. Ofcom proposes that all U2U services have:

- **Illegal Harms:** Systems or processes designed to swiftly take down illegal content of which they are aware. This is also a requirement under the OSA. Please see Ofcom's Statement here for more details.
- **Protection of Children:** Systems and processes to swiftly take down CHC. If children use the forum, or are likely to use it, it is Business A's responsibility to ensure they are prevented from seeing primary priority and are protected from priority content and non-designated content. Please see Ofcom's proposed approach here.

4.8. **Reporting and Complaints:** Effective reporting and complaints processes will also be necessary for Business A to ensure users can report the presence of illegal content or CHC. As elaborated in Ofcom's Illegal Content Codes and Protecting Children: Proposed Codes at a Glance, reporting and complaints functions should:

- Be easy to find, access and use;
- Acknowledge receipt and an indicative timeframe for a response/action; and
- Have clear processes/actions to be taken once a report/complaint is filed.

4.9. **Age Assurance:** The draft Protection of Children Codes proposed certain services use highly effective age assurance to prevent children from encountering primary priority content and protect them from priority content. This includes services with certain risks whose principal purpose is the dissemination of CHC, do not prohibit types of CHC in their Terms of Service, or operate recommender systems. Ofcom set out draft guidance on highly effective age assurance in Annex 10 of the protection of children consultation.

As noted above, if Business A maintains user profiles as public by default, children will be at heightened risk.

4.10. **High Privacy:** Standard 7 of the ICO's Age Appropriate Design Code specifically states that settings must be 'high privacy' by default. This means that children's profiles must be private by default, ensuring their information is only visible to other service users if the child amends their settings to allow this. This is because children may not fully understand the implications of having their profile set to public by default. As such, a private by default setting is a requirement for children, even in cases where adults have public by default profiles.

4.11. The decision to set user profiles to public by default must be balanced against the potential privacy and online safety risks. Any assessment to opt for a public by default approach should be included in Business A's children's access assessment, children's and illegal content risk assessments, and DPIA.

4.12. **The Recommendation for 'Private by Default':** One measure to mitigate harm is to implement a private by default setting for user profiles. This approach ensures a higher level of privacy and protection, with profiles visible only to other service users. Users could then actively choose to make their profile public if they wish. By making profiles private by default, Business A would likely reduce the risk of unintentional exposure, give users greater control over their personal data, and lessen the likelihood of exposure to harmful content.

5. What responsibilities do we have if we use AI to make health recommendations as "best suggestions" to users?

Summary

- Using AI to make health recommendations, including under the term "best suggestions" or similar, requires careful attention of the consumer protection, data protection, and online safety implications.
- Business A should particularly note banned practice 17 of the CPRs which prohibits falsely claiming that a product is able to cure illnesses, dysfunction or malformations. (5.1)
- Business A should review the CMA's AI Foundation Models Initial Review which identifies potential consumer protection concerns related to foundation models. (5.2)
- If Business A has considered its legal obligations and established that it will not infringe the CPRs by making health recommendations as "best suggestions" in these circumstances, it will need to produce a DPIA (5.3) and conduct risk assessments (5.4) to identify and mitigate data protection and online safety risks.
- When providing "best suggestion" to users:
    - Business A must ensure that the information it provides to users via health recommendations is not misleading. (5.5) Business A should consider and follow the recommendations set out in CMA guidance on the Trader Recommendation Platforms as it relates to user reviews to reduce the risk of infringing consumer law. (5.6)
    - Business A should document in its DPIA how it will maintain statistical accuracy of its recommendations and what steps it will take to moderate potentially harmful content. (5.7)
    - Business A should also not omit or hide 'material information' from its "best suggestions". (5.8)
    - Business A should consider the requirement that any terms with users about the use of its service are fair and transparent as required by the CRA. (5.9)
    - Business A should note that data protection law applies to all automated individual decision-making and profiling. (5.10)
- In addition to the below response, Business A should apply the advice provided in:
    - Question 2, for data protection guidance on special category data, purpose limitation, data minimisation, transparency and individual rights, to this processing activity.

- Question 3, for online safety guidance specific to illegal harms and protection of children.

Please note, Business A's queries appear to engage areas of the law, such as medical regulation and tort law, and raise broader ethical considerations that the DRCF regulators cannot provide informal advice on. Before releasing any service, businesses must ensure that it adheres to all applicable laws, guidance and rules, including by way of example approaches set by other relevant regulators such as the Medicines and Healthcare products Regulatory Agency ('MHRA'). We strongly advise seeking independent legal advice in this regard and encourage businesses to approach relevant authorities and regulatory bodies directly if appropriate.

Response

Should Business A decide to make health recommendations as "best suggestions", it will need to consider (amongst other things) the following:

5.1. **Claims about Curing Illness:** The CPR requirements are likely to apply where businesses use AI to make health recommendations to users as part of their commercial practice(s). The CPRs set out a list of commercial practices which in all circumstances are prohibited, irrespective of their effect or potential effect on the average consumer – Business A should note in particular banned practice 17 which prohibits falsely claiming that a product is able to cure illnesses, dysfunction or malformations. If untrue, any "best suggestions" which incorporate such claims would automatically infringe the CPRs and breach the law. Business A should especially consider the impact of its commercial practices on users who may be considered to be vulnerable consumers in this context, taking account of the nature of the recommendation and those who are likely to read it.

5.2. **AI and consumer protection:** The CMA refers Business A to its AI Foundation Models Initial Review, particularly Section 5 of the initial report, which identifies potential consumer protection concerns of foundation models. These concerns include fake reviews, false and misleading outputs, hallucinations, potential for user manipulation, hidden advertising. The report also notes the importance of ensuring that risks are identified and mitigated to avoid any harm to users of the AI system. The CMA published a set of six principles in its AI Foundation Models: Update Paper to help guide markets towards positive outcomes for UK businesses and consumers. The CMA urges all firms to align their business practices with the principles the CMA has set out.

Preparing the service

5.3. **Produce a DPIA**: If Business A has considered its legal obligations and established that it will not infringe the CPRs by using AI to make health recommendations as "best suggestions" in these circumstances, it must under data protection law produce a DPIA in order to identify and mitigate any data protection risks. As advised in Question 2, large-scale processing of health-related data, particularly when using AI, requires strong justification due to the sensitive nature of the data. The DPIA should clearly document the need for using AI specifically, showing that AI is an essential part of providing suggestions and cannot be accomplished in a less intrusive way.

The DPIA also needs to assess proportionality, weighing a business's interests in using AI against the risks to users' rights and freedoms. Business A will need to consider any risks to children or users with health conditions who may rely on these suggestions and outline mitigations. One measure could include flagging recommendations as AI-generated insights. Consider also how both the service

and users can label sensitive or harmful content for removal or human review. If such content is labelled, this content should not be recommended to further users.

5.4. **Conduct risk assessments and comply with safety duties:** As outlined in question 3, as a U2U service under the OSA, Business A must complete illegal content and children's risk assessments. If Business A is using a 'recommender system' to provide health recommendations to users, as defined in Ofcom's Illegal Content Register of Risk Glossary, the risk assessments will enable it to determine whether its recommender system poses high, medium, or low risk of illegal content and/or CHC.

- Additionally, both risk assessments include risk profiles for services with recommender systems, which highlight specific harms that Business A should be mindful of when implementing a recommender system. Ofcom has published its Illegal Content Codes, available here, and will publish its Protection of Children Codes in April. These Codes contain measures to help address the risks identified. Ofcom would advise Business A to consult these Codes, although services can choose other measures so long as they remain compliant with the duties.
- The illegal content risk assessment has been published and is available here. Services will have until March 2025 to complete the risk assessment. The children's risk assessment will be published in April 2025, and services will be expected to be completed by July 2025. As the children's risk assessments are being finalised, businesses can review Ofcom's quick guide here.

Providing "best suggestions" to users

5.5. **Misleading Practices:** If Business A provides false information to users in the form of recommendations and this causes or is likely to cause them to take a different decision as a result, it will engage in a misleading action under consumer protection law. Similarly, Business A should also ensure that the information forming the recommendation is not presented to users in a way that is likely to deceive them – even if the information presented is factually accurate. Business A should therefore be conscious when providing health recommendations of how users are likely to interpret what is said to reduce the risk of misleading them and infringing the law. See the unfair commercial practices guidance for more information on misleading practices.

As highlighted in 5.1, Business A should note banned practice 17 which prohibits falsely claiming that a product is able to cure illnesses, dysfunction or malformations.

5.6. **User Reviews**: Business A is ultimately responsible for the information which it publishes or otherwise makes available to consumers on the forum. Where third parties are sharing content on the forum, consumer law is likely to require Business A to take such appropriate steps as are necessary to ensure that users are not misled by 'reviews' from users of the forum or other third parties concerning opinions on or experiences of products (e.g. medicines), including where such reviews influence or determine recommendations. In addition to potentially engaging in a misleading commercial practice where Business A provides false or otherwise misleading information to consumers as part of its own "best suggestions", it may contravene the requirements of professional diligence and infringe the CPRs where it does not take such appropriate steps as are necessary to prevent and remove false or misleading information from third parties from publication – see for example Principle 6 of the CMA's compliance advice for Trader Recommendation Platforms (TRPs) which describes the practical steps which Business A may be required to take.

Note that the Government has recently introduced new 'banned practices' as part of the Digital Markets, Competition and Consumers Act 2024 which are expected to come into force in 2025. The new legislation will make it illegal, in all circumstances and irrespective of the potential impact on consumers, for businesses to submit or commission others to submit fake reviews or concealed incentivised reviews. Businesses that publish this content – including online forums – will also have an express legal responsibility to take such steps as are necessary to prevent and remove this false and misleading content from publication.

The representations (e.g. claims a business makes or impressions it gives) about a service or the quality, reliability or suitability of the reviews that appear on a forum are that business's responsibility and users should be able to trust this content. Business A should note the advice provided by the CMA for TRPs. The advice provided for TRPs is relevant for Business A to help it understand its obligations under the CPRs in relation to the activities of users of the forum. If Business A creates the perception or expectation that the information on its forum is trustworthy, reliable or suitable for a consumer's requirements, it should take note of the six compliance principles set out in the advice.

5.7. **Accuracy:** When handling health data, accuracy is critical. Ensuring personal data is correct and up-to-date is a fundamental principle of UK GDPR.

In the context of AI, accuracy also refers to Statistical Accuracy – the system's ability to consistently provide relevant and reliable suggestions. Because Business A's AI recommendations are based on popularity and similarity, there is a risk that high-engagement content may be prioritised, even if it is medically incorrect.

It is important for Business A to document in its DPIA how it will maintain statistical accuracy of the 'best suggestions' and what steps it will take to moderate potentially harmful content. In many cases, AI-driven suggestions should be treated as statistically informed guesses rather than factual information. The ICO recommends that Business A labels its "best suggestions" as AI-driven and highlight that they are based on trends or other users' experiences, not professional medical advice. Including this language in the output may help to manage users' expectations about the source of this information and reduce the likelihood of them relying on potentially harmful content. Please note that there will likely be separate, additional requirements and considerations under consumer law concerning misleading commercial practices (as described in this document).

5.8. **Material Information:** Similarly, under consumer protection law, Business A must also not omit or hide 'material information' from its "best suggestions". Material information should be provided in a clear and prominent way and in this context is likely to include (but is not limited to):

- How Business A will use users' information to generate "best suggestions"– including relevant information as to the limitations of that information;
- The fact that Business A uses AI to help generate such recommendations as "best suggestions", including a general description of how the AI does this/what it relies on and information on the limitations of the AI model; and
- Whether there has been any qualified medical review of the "best suggestion" (including reference to the reviewer and any relevant medical publications) and, that to the extent there has not, the fact that the information provided is not medical advice and does not come from a suitably qualified professional. This is in addition to Business A's legal obligation not to provide users with false information by, for example, describing a recommendation in a manner that gives, or is likely to give, users the impression that it is medical advice when this is not true.

5.9. **Fair and Transparent Terms**: Business A should also ensure that its terms with consumers for use of Business A's service are fair and transparent, as required by the CRA. As with the CMA's response to question three, Business A should note that the CRA also states that a trader cannot use its consumer terms or notices to restrict liability for death or personal injury resulting from its negligence.

5.10. **Automated Decision-Making:** Data protection law applies to all automated individual decision-making and profiling. Article 22 of the UK GDPR has additional rules to protect individuals if businesses are carrying out solely automated decision-making that has legal or similarly significant effects on them.

- This is crucial in the context of AI systems making health-related recommendations. For instance, if a user is recommended to view content about a medical issue based on another user's experience, and that content is medically inaccurate, it could lead to significant consequences. Business A must, therefore, assess whether its processing is subject to Article 22 of the UK GDPR, and if so, document within its DPIA how it meets the requirements. Business A may also find it useful to read the ICO's dedicated AI Toolkit, which provides comprehensive guidance on some key data protection risks and considerations when using AI.

Glossary

Relevant Regulator	Term	Description
ICO	**UK GDPR**	UK General Data Protection Regulation
	Lawful Basis	Under Article 6 of the UK GDPR, organisations must have a valid lawful basis to process personal data. Consent is one of six available lawful bases.
	Special Category Data	Special category data is personal data that needs more protection because it is sensitive. In order to process special category data, a business must identify both a lawful basis under Article 6 of the UK GDPR and a separate condition for processing under Article 9. Health data is an example of special category data.
	PECR	Privacy and Electronic Communications Regulations
	DPIA	Data Protection Impact Assessment
CMA	**CPRs**	Consumer Protection from Unfair Trading Regulations 2008
	Trader	A trader is a person acting for purposes relating to their business. The CPRs will apply to a trader's commercial practice if it is directly connected with the promotion, sale or supply of goods or services to or from consumers.
	DMCCA	Digital Markets, Competition and Consumers Act 2024, which will replace CPR when the relevant part of the legislation comes in force in 2025.
	CRA	Consumer Rights Act 2015
Ofcom	**OSA**	The Online Safety Act 2023 is a regulatory framework aimed at making online services safer for the people who use them by ensuring companies have effective systems in place to protect users from harm.
	U2U Service	User-to-user services are services where: • The service enables users to interact with one another, including by generating, uploading or sharing content, such as images, videos, messages or comments, with other users of the service; and • The service intends to have links with the UK

		○ by having either a significant number of UK users or the UK being a target market for the service as per section 4(5) of the OSA; or ○ by the service being capable of being used in the United Kingdom by individuals, and there are reasonable grounds to believe that there is a material risk of significant harm to individuals in the United Kingdom presented by user-generated content present on the service as per section 4(6) of the OSA.
	Search Service	Search service are services which are, or include, a search engine. A search engine is a service or functionality which enables users to: • Search at least more than one website and/or database; or • In principle, to search all websites and/or databases Please note that Generative AI (GenAI) models could constitute a search service where they enable the search of more than one website or database, for example via plug-ins. Search services will have separate duties they need to consider under the OSA.
	Codes	Codes of practice (Codes) are the set of measures recommended for compliance with relevant illegal content and protection of children duties. These are only recommended measures and services can choose other measures, so long as they remain compliant with their duties.
	Combined Service	A U2U service that includes a public search engine.
	Illegal content	As outlined in Section 59 of the OSA, illegal content is defined as "content that amounts to a relevant offence". Relevant offences comprise: • **Priority offences**, which are the most serious offences as defined by Parliament, and all services will need to act to prevent users encountering content amounting to one of these offences. They include offences of terrorism, offences relating to child sexual exploitation and abuse, and other offences. They are set out in Schedules 5-7 of the Act.

		• **Relevant non-priority offences**, which include other offences, subject to certain criteria. • **Inchoate offences**, which include offences of attempting or conspiring to commit a priority offence or relevant non-priority offence, or encouraging or assisting, aiding, abetting, counselling or procuring the commission of one of those offences. These offences have been outlined in the Illegal Harms Statement here.
	Children	Within the OSA, a child is defined as a person under the age of 18.
	CHC	**Content that is harmful to children (CHC)** includes three categories, outlined below: • **Primary Priority Content:** Prevent children of any age from encountering Primary Priority Content. This requires the use of highly effective age assurance unless the terms of service prohibit the relevant form of Primary Priority Content on the service for all users. • **Priority Content:** Protect children in age groups judged to be at risk of harm (in the risk assessment) from encountering Priority Content. • **Non-Designated Content:** Protect children in age groups judged to be at risk of harm (in the risk assessment) from encountering Non-designated Content Please see Table 3.1 for a list of CHC as per the OSA. Based on the type of content, it is a service's responsibility to take or use proportionate measures relating to the design or operation of the service.