DRCF AI and Digital Hub Example Query

Organisation A: We have developed a novel AI solution for online retail businesses. A business can upload a picture of the product it plans to sell, and the solution will describe its features and specifications (eg, colour, size and shape) using the picture. The solution can also tailor the product descriptions in real-time based on a shopper's browsing history. We have the following questions:

- Do we need the shopper's consent in using their browsing history to tailor the product descriptions? If so, is it our or the online shop's responsibility to obtain the necessary consent?
- Does the online shop need to make clear to the shoppers that the product descriptions are written by AI and what information the AI relies on to do this? What information will we consequently need to provide to them on how the AI operates?
- We are committed to responsible AI development and are aware of the risk of the AI writing offensive or misleading product descriptions. Can we contact our competitors and work together to address the issue?

DRCF AI and Digital Hub Example Response

Introduction

Thank you for submitting your Query to the DRCF AI and Digital Hub ('Hub').

Your Query has been responded to by the following DRCF Regulators ('we', 'us', 'our'):

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

Our informal advice is provided to you in line with the Conditions for Participation.

Our informal advice is provided to you based on our current understanding of the legal and regulatory frameworks within our remits and how they apply to your product/service. Our informal advice should not be treated as an exhaustive account of the issues linked to your product/service or represent an endorsement of your proposed innovation.

Our informal advice is provided to you only and is specific to your circumstances as described by you in the information you provided to the Hub. Our informal advice must not be shared with any other party (either in part or in full) without our express permission. This does not prevent you from disclosing our informal advice to your legal advisers or auditors provided that you highlight this disclaimer and the Conditions for Participation when doing so.

Our informal advice is provided to you without prejudice to any future regulatory intervention by any DRCF or non-DRCF regulator and nor is it a substitute for independent legal advice which you may wish to seek in advance of the launch of your product/service.

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

Please note, a separate case study based on our informal advice may be published. We will consult you shortly on the content of the case study and give due regard to any confidentiality concerns.

Your Query

We understand your target market are businesses in the retail sector and that you are seeking advice on providing your AI solution to those businesses. The AI solution enables a business to upload a picture of the product it plans to sell, and the solution will describe its features and specifications (eg, colour, size and shape) using the picture. The solution can also tailor the product descriptions in real-time based on a shopper's browsing history. Your questions are:

- Do we need the shopper's consent in using their browsing history to tailor the product descriptions? If so, is it our or the online shop's responsibility to obtain the necessary consent?
- Does the online shop need to make clear to the shoppers that the product descriptions are written by AI and what information the AI relies on to do this? What information will we consequently need to provide to them on how the AI operates?
- We are committed to responsible AI development and are aware of the risk of the AI writing offensive or misleading product descriptions. Can we contact our competitors and work together with them to address the issue?

Summary of our response

- Using a consumer's browsing history to tailor product descriptions involves processing personal data. The responsibility for determining the appropriate lawful basis for this processing rests with the controller, which is likely to be the online retailer. However, depending on the specific circumstances you could be joint controllers.
- When consent is used as the lawful basis, the controller (or joint controllers, where relevant) is responsible for obtaining consent from consumers in accordance with the UK General Data Protection Regulation ('UK GDPR'). It can be a challenge to obtain valid consent under UK GDPR. Strict rules apply. Consent must be freely given, specific and informed, and you need to maintain records to demonstrate you have obtained valid consent.
- Transparency is a key principle of UK GDPR. Controllers are required to provide consumers with clear and transparent information about how they will process their personal data. Given that tailoring product descriptions involves the processing of personal data, this should be made clear to consumers before any processing begins.
- As regards the use of AI to create the product descriptions, it is essential to inform consumers of the potential implications of using AI, such as the possibility of errors or biases in the product descriptions. Consideration must also be given to whether the use of AI in this context involves solely automated decision-making or profiling and whether that is likely to have a significant impact on an individual's behaviour.
- Where you supply your AI software to online retailers and they use your product as part of the promotion, sale or supply of products to consumers (eg, to create personalized product descriptions), those businesses must comply with consumer law – in particular the Consumer Protection from Unfair Trading Regulations 2008 (CPRs).
- You should also note that where you are selling your product to other businesses the Business Protection from Misleading Marketing Regulations 2008 (BPRs) prohibit you from giving misleading information to another business that would deceive that business and affect, or be likely to affect, its economic behaviour.
- You asked whether you might collaborate with competitors to address the risk of the AI in your product writing offensive or misleading descriptions. The exchange of information between competitors may infringe Chapter I of the Competition Act 1998 where it has the potential to remove or reduce competitive uncertainties and/or may influence the competitive strategy of the competing businesses. However, it is recognised that certain information exchanges can be pro-competitive or competitively neutral (and therefore fall outside the scope of the Chapter I prohibition altogether). The CMA's Horizontal Guidance sets out a number of factors you should consider to assess compliance.

1. Lawful Basis and Consent

Do we need the shopper's consent in using their browsing history to tailor the product descriptions? If so, is it our or the online shop's responsibility to obtain the necessary consent?

To answer this question, you must first identify the personal data that will be processed and determine who acts as the controller in your relationships with the online retailers. This is crucial because the responsibility for selecting the appropriate lawful basis for personal data processing sits with the controller. It is important to note that consent is just one of six available lawful bases. Below, you will

find a step-by-step guide on how to establish responsibility and controllership, followed by advice on selecting the appropriate lawful basis.

The UK GDPR applies only to personal data. As a first step, you must assess and document the personal data you will process as part of your AI solution. Personal data is any information relating to an identified or identifiable natural person.

While the product descriptions themselves may not qualify as personal data, tailoring these descriptions based on a consumer's browsing history likely does involve the processing of personal data.

Once you have worked out the personal data that you will be processing, you should map out how this data flows between your system and the online retailers you collaborate with, and maintain detailed records of these flows. Our "What is Personal Data" guidance may help you to distinguish between personal and non-personal data.

After identifying the personal data and creating a data flow map, the next step is to determine the responsibility for processing personal data.

The UK GDPR distinguishes between a 'controller' and a 'processor' to recognise different degrees of responsibility. A controller makes decisions about processing activities, exercises overall control of the personal data being processed and is ultimately responsible for the processing. In contrast, a processor acts on behalf of and in the interests of a controller. The processor follows the controller's instructions as the controller is the organisation that determines the purpose and means of processing.

When establishing controllership between you and the online retailers, several factors should be taken into account, including the degree of independence you exercise and what role you play in determining the means and purpose of processing. You need to break down the processing into separate processing activities and make an assessment of the role each organisation plays in relation to each processing activity. It is important to note that organisations are not by their nature either a controller or a processor. Instead, the personal data and how each organisation uses it will need to be considered when making an assessment. Our Controllers and Processors guidance outlines the key considerations for establishing controllership.

It is possible that your organisation will be a controller if you use personal data to train the AI software, although this will also depend on where you obtain the training data from and what rights you have to use that data.

In terms of the online retailers using your software, it will depend on the nature of the relationship you have with them as to whether you are a controller, joint controller or processor. You will need to examine each relationship and processing activity individually.

Your role may change at different stages of the processing operation. For example, you may be a processor when providing your AI service to online retailers when your AI solution is used to generate product descriptions for their consumers, but revert to a controller if you use personal data for any separate purposes which are specific to you. Special attention should be paid if you fine-tune your AI based on a retailer's consumer interactions with your software.

You should outline your established role on a case-by-case basis with the online retailers.

If you are a processor, you and the online retailers/controllers must ensure that there are appropriate Contracts in place in accordance with Article 28 UK GDPR, which set out clear instructions of how you are to process personal data. You must make sure the contract includes sufficient detail about your AI

service and contains contractual assurances so that the online retailer can verify and evidence its compliance as a controller with UK GDPR. If sufficient information is not provided, you may be a controller or joint controller, as the online retailers may have a limited understanding of the personal data processing taking place.

Joint controllers are required by Article 26 UK GDPR to enter into a formal agreement setting out agreed roles and responsibilities, this includes specifying which controller is the contact point for consumers to exercise their individual rights.

If you are sharing data as separate controllers, it is good practice to enter into a Data Sharing Agreement ('DSA'), as outlined in our Data Sharing Code. These agreements should set out the role and responsibilities of each organisation, such as outlining what each organisation should do when an individual rights request is received. Each controller must also ensure they are complying with Articles 13 and 14 UK GDPR. This means providing consumers with information about how their personal data is processed and by whom. See below under the heading 'ICO response on transparency' for further information.

Once you have determined the appropriate controllership, you can move on to consider the appropriate Lawful Basis for each processing activity of personal data under Article 6 UK GDPR.

A lawful basis is essentially the reason for processing personal data. Consent is one of six available lawful bases. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on the nature of your organisation, your purpose for processing and relationship with the individual whose data is being processed.

The responsibility for determining the lawful basis sits with the controller. In this context, if you are only carrying out processing activities on behalf of the online retailer and all of your processing is sufficiently described within an Article 28 UK GDPR contract, then it is likely that the online retailer will be the controller and you the processor.

Consent is the most appropriate lawful basis if the controller wants to provide consumers with genuine choice and control over their personal data. For tailoring product descriptions based on browsing history, consent could therefore be a suitable lawful basis as it should offer consumers a real choice in terms of how you analyse their personal preferences and online behaviour.

Other lawful bases are less applicable in this context. However, Legitimate Interests could be considered. This lawful basis requires carrying out a 'legitimate interests assessment' which requires the controller to balance the controller's need to process personal data against the individual's rights and interests as part of the three part test.

Since the tailoring of product descriptions is not essential for the consumer to view, understand or purchase a product, but instead is intended to enhance the shopping experience, the controller would need to justify any impact of the processing on the consumer and ensure any risks to the consumer's interests are proportionate. One way of assisting with the balancing test would be to provide an easy way for consumers to object to this processing, which could be managed via a simple opt out. However, care would need to be taken to ensure the processing did not fall within Article 22 UK GDPR processing by having a significant impact on consumer's behaviour (this is covered in more detail in Question 2).

Assuming consent is used as the lawful basis, the controller must also consider several other factors.

- Clear and unambiguous consent – consent must be an active, affirmative action by the consumer, indicating a clear opt-in. Pre-ticked boxes or default consent mechanisms are not

compliant with UK GDPR. Consumers should be presented with a straightforward, binary choice, ensuring that they understand what they are consenting to.

- Specific and granular consent – consent requests should be specific and granular, meaning that consent for one processing activity (eg using browsing history to tailor product descriptions) must be separate from other activities (eg targeted advertising). Bundled consent undermines the consumer's control over their data, which is why each consent request should stand on its own.
- Transparency – when obtaining consent, transparency is key. Consumers must be fully informed about what their consent means – who will have access to their personal data, how long the data will be retained, and for what specific purposes it will be used. This information must be conveyed in clear, plain language.
- Ease of withdrawal – consent must be as easy to withdraw as it is to provide. The withdrawal process should be simple, accessible, and immediate, without any penalties for the consumer. For instance, if a consumer decides to withdraw consent, this action should be executable with a single step.

2. Consumer protection and transparency considerations

Does the online shop need to make clear to the shoppers that the product descriptions are written by AI and what information the AI relies on to do this? What information will we consequently need to provide to them on how the AI operates?

ICO response on transparency

Under Articles 13 and 14 UK GDPR, consumers have the Right to Be Informed about the collection and use of their personal data. This transparency requirement is fundamental, ensuring that processing activities are clear, open, and honest from the outset.

Transparency involves clearly communicating to consumers who you are, the purposes for processing their personal data, the lawful basis for doing so, retention periods, and any third parties with whom the data will be shared. This information must be provided at the time of data collection and must be concise, intelligible, and easily accessible, using plain and clear language.

Typically, this information is delivered through a privacy notice, which should be regularly reviewed and updated as necessary. If new uses of a consumer's data arise, the controller must notify them before starting the new processing activities. In this context, this means that the controller (or joint controllers) must inform consumers about how their personal data (eg browsing history) will be used and, in particular, the role of AI in the process, before the processing begins.

If personal data is shared with other organisations, it is crucial to inform consumers of this as part of transparency obligations. You must be specific to whom the data will be disclosed, either by naming the organisations directly or by categorising them in a way that provides meaningful information.

When using AI to tailor product descriptions, it is essential to inform consumers of the potential implications, such as the possibility of errors or biases in these descriptions. This is particularly important given the profiling activities that may occur as part of your AI's functionality.

You will need to assess whether the processing involving the AI solution involves profiling. This is defined under Article 4(4) UK GDPR, as any automated processing of personal data intended to evaluate personal aspects of an individual, including their preferences, interests or behaviour. Profiling

activities in your AI solution could include analysing browsing history to predict and tailor product recommendations.

You are engaged in profiling if you:

- Collect and analyse personal data on a large scale using algorithms, AI or machine learning.
- Identify associations to build links between different behaviours and attributes.
- Create profiles that you apply to consumers.
- Predict consumers' behaviour based on their assigned profiles.

Automated Decision-Making is the process of making a decision by automated means without any human involvement. These decisions can be based on factual data, as well as on digitally-created profiles or inferred data. Automated decision-making often involves profiling, but it does not have to.

It is the responsibility of the controller to ensure consumers are aware of when such processing may take place.

You also need to be aware of the application of Article 22(1) UK GDPR which limits the circumstances in which you can make **solely automated decisions**, including those based on profiling, that have a **legal or similarly significant effect on consumers**.

If, by providing tailored product descriptions based on browsing history you encourage or influence consumers to make expensive purchases, you would need to consider whether this is having a significant impact on the consumer's circumstances, behaviour or choices.

CMA response on consumer protection, including transparency

The following sets out considerations for complying with consumer protection law.

Where you supply your AI software to online retailers and they use your product as part of the promotion, sale or supply of products to consumers (eg to create personalised product descriptions), those businesses must comply with consumer law – in particular the Consumer Protection from Unfair Trading Regulations 2008 **(CPRs)**. For example, they will be responsible for:

- Ensuring that the AI-generated information they provide to consumers about products they are promoting, selling or supplying is accurate and not false or in any way likely to deceive consumers.
- Depending on the nature of the output, providing all 'material information' which consumers need to make an informed decision about whether, how or on what terms to purchase a product from that retailer. What information is 'material' will depend on the circumstances (eg the audience to whom the product is being marketed) and the nature of the product being promoted, sold or supplied – but in this context this may include i) the fact that the descriptions they are seeing have been tailored by AI based on the consumer's browsing history, and ii) a general description of how the AI uses the information in consumers' browsing history to generate what they are seeing (and the extent to which the consumer can control this).

Even where you as the supplier of the AI software do not have any dealings with consumers, consumer law will apply to you where your activities are 'directly connected' with the promotion, sale or supply of products to or from consumers. The courts have interpreted this phrase broadly. Depending on the specific context and content of your practice, where you have designed and trained your AI product to

enable or facilitate the sale of products to consumers, this test may be met. Accordingly, you must take steps to ensure that your own practices comply with the CPRs:

- First, you must ensure that you do not engage in a misleading practice by, for example, designing or training your AI tool to provide false information or in any way deceive consumers.
- Further where you are engaged in a commercial practice you must not contravene the requirements of 'professional diligence' – that is, the standard of special skill and care which a trader may reasonably be expected to exercise towards consumers which is commensurate with either honest market practice or the general principle of good faith in your field of activity. 'Consumers' is interpreted broadly and extends to consumers who do not make purchases directly from you. While it can be difficult to pinpoint responsibility for a particular failure, to the extent that your product is intended to be used by someone else to promote, sell or supply products to consumers, you should consider what steps may be necessary to ensure that your generative AI product does not harm end consumers by distorting their economic behaviour (see for example paragraphs 133-142 in the CMA's Response to Price Transparency Consultation). For example, this may include proactive steps to identify, assess and address the systemic risks of harm to consumers which might arise from the use of your software, and consider whether you are providing sufficient information to your online retailers so that they can comply with their own legal obligations when using your product – for example providing online retailers with sufficiently detailed information about the performance and functionality of your model, how it utilises consumers' browsing history to determine what they see and the requirement to take steps that are necessary to ensure that consumers are provided with truthful and accurate information about products.

You should also consider referring to the CMA's AI Foundation Models Report (in particular paragraphs 6.7 to 6.12), which sets out the CMA's general views on compliance with the CPRs and other consumer law matters (eg unfair terms law), and reiterates the CMA's position that consumer law can also apply to suppliers (as well as end users).

Where you are selling your product to other businesses, the Business Protection from Misleading Marketing Regulations 2008 ('BPRs') prohibit you from giving misleading information to another business that would deceive that business and affect, or be likely to affect, its economic behaviour. This includes giving false information about your AI software's inputs or how it works to produce content for consumers.

Finally, alongside ensuring that you are complying with current law, you and the online retailers should be mindful of upcoming legislative changes. The new Digital Markets, Competition and Consumers Act received Royal Assent on 24 May 2024 and, while the relevant provisions are not yet in force, the Act will replace and update the CPRs. The CMA will be publishing guidance to explain the application of the new law and what businesses should do to comply in due course. In the meantime, you should seek separate legal advice if you consider that these circumstances could apply to you - your proposal is likely to require a careful examination of various factors, including those set out above.

3. Competition considerations when working with competitors

We are committed to responsible AI development and are aware of the risk of the AI writing offensive or misleading product descriptions. Can we contact our competitors and work together with them to address the issue?

You asked whether you might collaborate with competitors to address the risk of the AI in your product writing offensive or misleading descriptions. We note that such collaboration would likely involve the sharing of information among competitors.

A key principle of competition law is that each business should determine independently its economic conduct on the market. The exchange of information between competitors may infringe Chapter I of the Competition Act 1998 where it has the potential to remove or reduce competitive uncertainties and/or may influence the competitive strategy of the competing businesses. Whether or not the exchange of information may infringe competition law will depend on the circumstances of the individual case, including the market characteristics (eg more problematic if the market is concentrated with only a small number of AI developers), the type of information exchanged (eg more problematic if the exchanged information in question is current/future planned, granular and/or relates to pricing, customers and pipeline products) and the way it is exchanged (eg more problematic if the exchanges in question are frequent and only involve certain businesses to the exclusion of others). It should be noted that these factors (and others) would be considered in the round and the more factors that are engaged, the more problematic and concerning the arrangement is likely to be.

In the most serious and concerning cases (eg sharing information about your future pricing intentions), information exchange between competitors is deemed anticompetitive by its very nature, meaning that the CMA will not have to show that the exchange has restrictive effects on competition.

Nevertheless, it is recognised that certain information exchanges can be pro-competitive or competitively neutral (and therefore fall outside the scope of the Chapter I prohibition altogether). Even information exchange that is otherwise problematic may be justified on the basis that it leads to 'efficiency gains', provided that the exchanges are reasonably necessary, the gains are passed on to consumers and the information exchange does not lead to the elimination of competition. In this case, for example, you might assess whether the 'efficiency gains' consisted in finding a solution to counter the generation of offensive or misleading descriptions by AI solutions, facilitating consumer choice, safety and certainty, and whether the envisaged information sharing is necessary for that endeavour.

In practice, you should consider, among other things, the following matters:

- If there is an alternative to the information exchange in question to solve the problem you are dealing with (ie. preventing the AI from producing false or misleading information), then it may be advisable to use that (eg to consult with an appropriate body such as a university or the AI Standards Hub which may already have a technical solution and may be able to answer your query).
- Whether the initiative and/or its outcomes are accessible to all AI developers (which is less likely to be problematic) or are instead restricted to a subgroup and, if so, the basis on which membership of such subgroup is determined.
- Whether any information exchanged is limited to aggregated, anonymised and historic data (which is less likely to be problematic), as opposed to current, granular data that, for example, identifies customers.
- Whether any information exchanged goes beyond what is necessary for the purpose (eg on the basis of what you have explained, there appears to be no need to disclose pricing information or commercial arrangements with customers).
- Whether any information exchanged will be first received and processed by a 'clean team' of individuals (eg in-house counsel) that are not involved in commercial operations and are

bound by strict confidentiality obligations with regard to that information or a neutral/independent third party.

It is not clear from your question whether you envisage developing an industry-wide technical standard as part of developing this product. If so, further considerations would come into play. This is a complex area that requires further detailed analysis, which we have not addressed in this response. For more information on standardisation agreements, see the relevant sections of the CMA's Horizontal Guidance such as chapter 9 on standardisation agreements.

Overall, we would advise you to consult the CMA's Horizontal Guidance and seek separate legal advice as its proposal requires a careful examination of various factors, including those set out above.

Further considerations

You should also note that the above considerations are not an exhaustive list of all considerations around processing consumers' browsing history to tailor product descriptions. For example, we highly recommend reading the ICO and CMA joint paper on Harmful Design in Digital Markets. This paper provides additional insights into considerations for designing online services and could be useful for your discussions with online retailers.