Date informal advice provided: 10 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:

Data protection and consumer law for businesses supporting SMEs to deploy AI

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'); and
- Competition and Markets Authority ('CMA')

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 nor is it a substitute for independent legal advice which a business may wish to seek in advance of the launch 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.

A non-confidential version of the informal advice provided to the applicant is attached to this case study. This informal advice was provided on 10 December 2024 and represents the position as at 10 December 2024. Businesses should consult relevant information and guidance on regulators' websites to keep up to date with the latest developments.

Date informal advice provided: 10 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

Query submitted to the Hub

Business A is a B2B service that helps SMEs harness the power of AI by connecting them with foundation models for the purpose of using chatbots (and other AI powered services such as object recognition and automation). Business A's purpose is to make it easy for SMEs to integrate AI into their operations. Business A would like to know what are the key considerations to be aware of when engaging different foundation model suppliers based in the EU, China and the US?

- Business A should map out where personal data may be processed between the various organisations involved. (1)
- Business A should carry out due diligence with foundation model suppliers and establish contracts with them that include appropriate data protection provisions. (2)
- Business A will be either a joint controller or processor for any personal data processed between them and their SME clients. (2)
- If business A shares personal data outside of the UK, it must ensure the processing complies with the international transfer rules. (3)
- Business A may have consumer protection responsibilities. Where business A integrates AI into an SME business and the SME uses business A's product as part of the promotion, sale or supply of products to UK consumers, those businesses must not engage in unfair commercial practices concerning consumers. (4)
- Even where business A, as a B2B service, does not have any dealings with consumers, consumer law will apply where business A's activities are 'directly connected' with the promotion, sale or supply of products to (or from) consumers. In particular, business A:
    - should ensure that they do not engage in a misleading commercial practice; and
    - must not contravene the requirements of professional diligence. (4.4)
- Business A is prohibited from giving misleading information to its SME clients that would deceive that business and affect, or be likely to affect, their economic behaviour. (4.6)

Date informal advice provided: 10 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

Introduction to the regulators

This query has been responded to by the ICO and CMA. 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 UK General Data Protection Regulation ('UK GDPR'), which is relevant to this informal advice.

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 ('CPR')[1]; and
- Business Protection from Misleading Marketing Regulations 2008 ('BPRs').

Regulator Response References

In the below table, we have set out the relevant regulator and the respective responses that they have input on. Each regulator is only responsible for the responses within their regulatory remit as noted in this table.

Regulator	Question	Relevant Responses
ICO	Q1	1-3.5
CMA	Q1	4-4.8

[1]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.

Date informal advice provided: 10 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

Response

1. Personal Data

1.1 To understand the key data protection risks and considerations relevant to business A's AI service, they should first identify if and where personal data may be processed by their organisation, the foundation model suppliers, and the SMEs they work with. While business A's service might not require personal data to function, personal data belonging to an SME's customers will likely be processed. For example, if an SME's customer enters personal data into a chatbot.

1.2 To help business A with this, the ICO recommends creating a personal data flow map to illustrate how personal data moves between the foundation model suppliers, their service, and the SMEs. This will help business A identify where personal data is processed and assign responsibilities. The ICO's 'What is Personal Data' guidance may help with this.

1.3 In addition, as business A intends to provide an AI service, they should consider the ICO's guidance on producing a Data Protection Impact Assessment ('DPIA'), Data Protection and AI, and its dedicated AI Toolkit, to help them assess their compliance with some of the key requirements under data protection law.

2. Controllers and Processors

2.1 Once business A has mapped out the flow of personal data, it is crucial to establish who is responsible for what under data protection law. The roles are:

- Controller: The organisation that decides why and how personal data is processed.
- Joint Controller: Two or more organisations that jointly decide why and how personal data is processed.
- Processor: The organisation that processes personal data on behalf of the controller, following its instructions.

2.2 Determining these roles depends on the nature of the processing, the context, and who has control over the data.

2.3 The ICO understands that it is not business A's intention to share any information, including personal data, with foundation model suppliers after procurement. However, it is still important to carry out and document appropriate due diligence before procuring their models. This means establishing contracts with appropriate data protection provisions that outline the responsibilities and degree of control each party has over the model and any data used in its development, including personal data.

2.4 It is also important to ask the foundation model suppliers about any usage restrictions and the measures in place to ensure accuracy and security. Business A should ask about the data used to train the model and request assurance that the supplier

complies with UK data protection law, including having a Lawful Basis for processing any personal data used for training.

2.5 Assessing the statistical accuracy of a foundation model is also key. Consider whether the training data and the model aligns with the needs and use cases of business A's SME clients. For instance, a model trained predominantly in one language (eg. Chinese) may be less effective in another (eg. English), resulting in lower accuracy or incomplete responses for end customers.

2.6 Given business A's role in integrating AI into SMEs' business operations, it is also important to define and communicate its data protection role with them, especially as business A's SME clients may not have the expertise or resources to fully understand and manage any AI-related risks. In most cases, business A will likely be acting as a processor or a joint controller alongside their SME clients when processing personal data. If a business has control and influence over 'why' (purposes) and 'how' (means) personal data is processed, they may be a joint controller, which would require a formal agreement with their clients outlining the roles and responsibilities, including specifying who is the point of contact for customers exercising their data protection rights. Businesses should review the ICO's guidance on Controllers and Processors to help determine their role and any subsequent steps to take.

3. International Transfers

3.1 Although business A indicated no current plans to share personal data with foundation model suppliers, it is still important to note that if they do decide to share personal data with any third parties outside the UK (including cloud providers), they must ensure that they follow the rules around international transfers, no matter how small or infrequent they are.

3.2 If business A is the responsible party for sharing the personal data, they will need to firstly consider if the transfer is to a country that has 'adequacy' status. This means that personal data can be transferred without further safeguards or additional conditions. This includes the EU member states like France, Germany and Spain, as well as the EFTA states (Iceland, Norway and Liechtenstein).

3.3 For the United States, there is a partial adequacy agreement in place under the UK Extension to the EU-US Data Privacy Framework. Business A will need to check if their transfers fall under this framework. There is Factsheet for UK Organisations on Gov.uk and further guidance on the US Department of Commerce's Data Privacy Framework Program Website.

3.4 For China, transfers are more complex as there is no 'adequacy' agreement in place. Business A would need to put in place additional safeguards to ensure the personal data is protected. This could include legal agreements or extra security measures. A

transfer risk assessment would also be required to ensure the data is protected once it is in China. This assessment involves looking at China's laws and seeing whether they undermine the protections offered under UK data protection law.

3.5 Please see the ICO's guidance on the International Transfers for further information.

4. Consumer Protection

4.1 The examples given in the CMA's response below are for indicative purposes, and whether a particular practice breaches consumer law will require a case-by-case assessment based on the particular facts and circumstances. The CMA does not cover every situation or practice in which a breach of the Consumer Protection from Unfair Trading Regulations 2008 (CPRs) may occur. This informal advice is not a substitute for independent legal advice, and should not be relied on as such.

4.2 Business A should be aware that they may have responsibilities under consumer protection law. Businesses are prohibited by the CPRs from engaging in unfair commercial practices concerning consumers. 'Commercial practice' covers any act, omission, course of conduct, representation or commercial communication by a business which is directly connected with the promotion, sale or supply of products or services to or from consumers. 'Consumer' means an individual acting for purposes that are wholly, or mainly, outside that individual's business.

4.3 Where business A integrates AI into an SME business and the SME uses their product as part of the promotion, sale or supply of products to UK consumers, those businesses must comply with the CPRs. This is the case regardless of which country specifically any foundation model has been developed. For example, business A's SME clients will be responsible for:

- Ensuring that any information generated by AI which is provided to consumers about products they are promoting, selling or supplying is not false or untruthful, or in any way likely to deceive the average consumer whom the information reaches or to whom it is directed or addressed.
- Depending on the nature of the output, providing all 'material information' which consumers need in order to make an informed decision about whether, how and on what terms to purchase a particular product. In this context, what information is 'material' will depend on the circumstances and the nature of the product being promoted, sold or supplied. 'Product' has a broad definition under the CPRs and includes goods, services or digital content.

4.4 Even where business A, as a B2B service, does not have any dealings with consumers, consumer law will apply to them where their activities are 'directly connected' with the promotion, sale or supply of products to (or from) consumers. The courts have interpreted this phrase broadly. This means that, depending on the specific context and content of business A's SME clients' practice, where their service involves

integrating a foundation model into business A's SME client's business to enable or facilitate the promotion, sale or supply of products to consumers, their practice may be 'directly connected' with that activity and they will therefore have responsibilities under consumer protection law even though consumers do not purchase directly from business A. If this is the case, business A must take steps to ensure that their own practices comply with the CPRs. In particular:

- Business A must ensure that they do not engage in a misleading commercial practice. This may be the case where, for example, during integration of a foundation model, they design or train it to provide false information or in any way deceive consumers. Where this causes or is likely to cause the average consumer to take a decision they would not have taken otherwise – for example, to purchase a promoted product - this is likely to infringe the CPRs.
- Business A must also not contravene the requirements of 'professional diligence' which is the standard of special skill and care which it may reasonably be expected to exercise towards consumers which is commensurate with either honest market practice or the general principle of good faith in their field of activity. Where business A does not exercise professional diligence and this causes the average consumer to take a decision they would not have taken otherwise, this is likely to infringe the CPRs.

4.5 While it can be difficult to pinpoint responsibility for a particular failure, to the extent that a foundation model is intended to be used by business A's SME clients to promote, sell or supply products to consumers, they should consider what practical steps may be necessary to ensure that the foundation model they connect them with does not harm consumers by distorting their economic behaviour (see for example paragraphs 133-142 in the CMA's Response to Price Transparency Consultation). This may include, amongst other things, taking proactive steps to identify, assess and address the systemic risks of harm to consumers which might arise from the use of a foundation model, and considering whether and if so, how business A can provide sufficient information on the foundation model to their SME clients so that they can comply with their own legal obligations when using business A's product. This could include providing business A's SME customers with sufficiently detailed information about the performance and functionality of a model to ensure that consumers are provided with accurate, truthful and complete information to enable them to take informed decisions.

4.6 Similarly, business A should consider the Business Protection from Misleading Marketing Regulations 2008 ('BPRs') which prohibit them from giving misleading information to their SME clients that would deceive that business and affect, or be likely to affect, their economic behaviour.

4.7 Business A should also consider the CMA's AI Foundation Models: Initial 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 protection legislation (eg. unfair terms

law). The CMA published a set of six **principles** in our Update Paper to help guide markets toward those 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.

4.8 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.