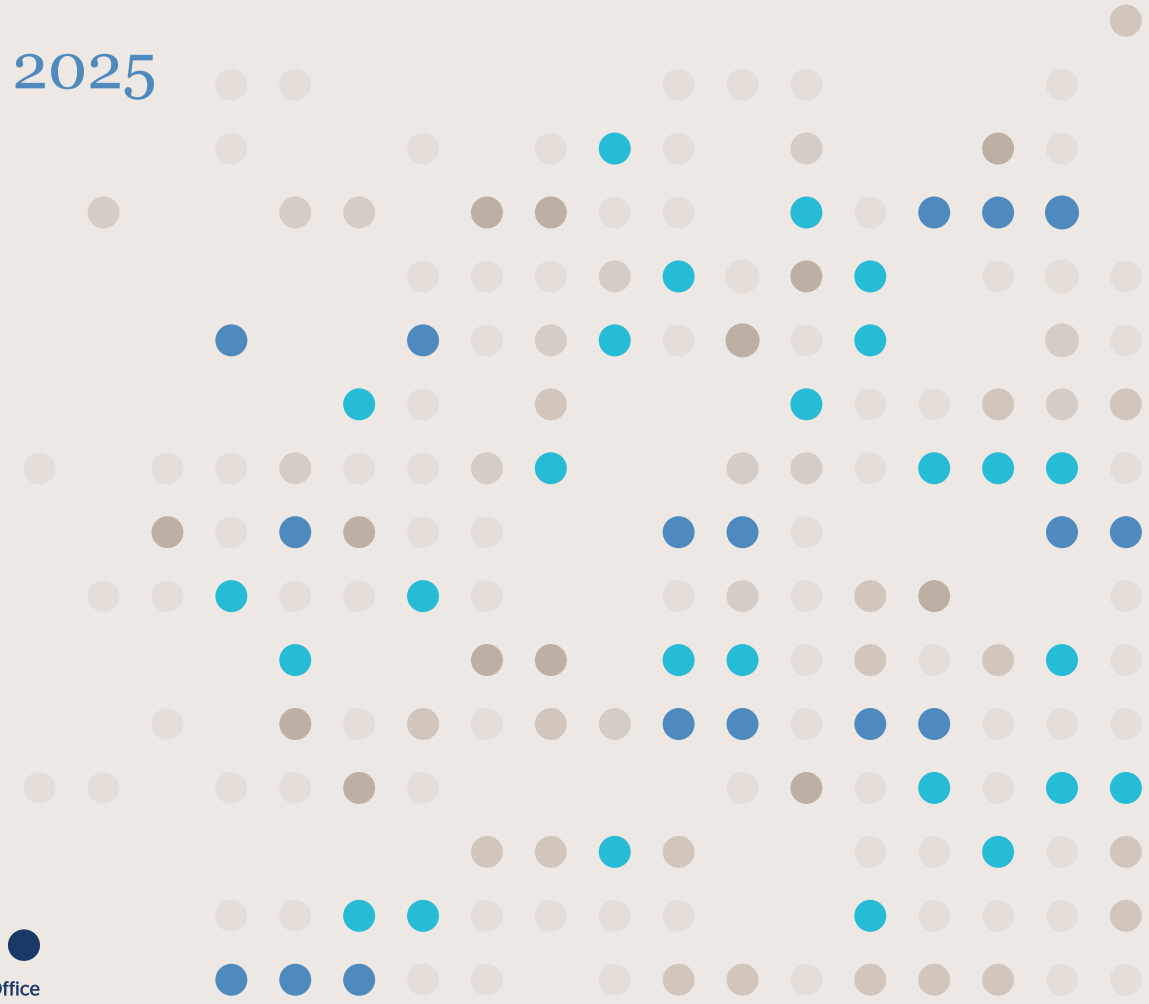
Information Commissioner's Office

Consent or pay Summary of call for views

January 2025



ico.
Information Commissioner's Office

Contents

1. Introduction

In March 2024, the Information Commissioner's Office (ICO) launched a call for views on "consent or pay" business models. This document provides a summary of the key themes from the responses we received and sets out how these have been considered and used to inform the ICO's consent or pay guidance.

We thank everyone who provided a response for their time taken to comment and share their views.

1.1. Context

"Consent or pay" refers to a business model for funding online products and services. This model gives people a choice to:

- consent to an organisation using their personal information for personalised advertising in order to access a product or service (**"consent to personalised advertising"**);
- pay a fee to access the product or service and avoid their personal information being used for personalised advertising (**"pay to avoid personalised advertising"**); or
- leave, or decide not to use the product or service.

Whilst "consent or pay" models have existed for some time, we have observed a recent uptake of these models both in the UK and globally. This has happened in the context of regulatory activity in the UK and abroad, industry developments, and changing expectations of consumers.

Any business practice involving the processing of personal data, including the funding model, must comply with data protection law. Where organisations are relying on consent as a lawful basis for processing people's personal data, including for personalised advertising, they must be able to demonstrate that people have freely given their consent. The ICO has published detailed guidance on consent which organisations should take into account when they rely on this lawful basis for processing people's personal information.

In our call for views, we explained that data protection law does not prohibit "consent or pay" business models. If an organisation chooses to adopt a "consent or pay" model they must be able to demonstrate that people can freely give their consent to the processing of their personal information for personalised advertising.

Our "consent or pay" guidance sets out a set of factors to support organisations assess whether a "consent or pay" model meets the standard

of consent. It is an organisation's responsibility to document and be able to justify how their "consent or pay" model is compliant with UK GDPR and the Privacy and Electronic Communications Regulations (PECR), taking into account the factors set out in this guidance.

1.2. ICO call for views

In March 2024, we published a call for views to hear from consumers and other stakeholders about "consent or pay" models. We sought views on our emerging thinking about how to consider the validity of consent in these models. We have used the responses to inform the development of our "consent or pay" guidance. Our emerging thinking set out that:

> data protection law does not prohibit businesses models that involve consent or pay. However, any organisation considering such a model must be careful to ensure that consent to processing of personal information for personalised advertising has been freely given and is fully informed, as well as capable of being withdrawn without detriment.

We set out four factors that organisations should consider when assessing whether people could freely give their consent:

Power balance[1]

To what extent is there a clear imbalance of power between the service provider and its users? Consent for personalised ads is unlikely to be freely given when people have little or no choice about whether to use a service or not, which could be the case when they are accessing a public service, or the service provider has a position of market power.

Appropriate fee

Is the fee appropriate? Consent for personalised ads is unlikely to be freely given when the alternative is an unreasonably high fee. Fees should be set so as to provide people with a realistic choice between the options, with the provider capable of providing objective justification of the appropriateness of the level.

Equivalence

Are the ad-funded service and the paid-for service basically the same? For example, if a service provider offers a choice between personalised ads and a "premium" ad-free service that bundles lots of other additional extras together, then this wouldn't be the case.

[1] During the call for views this factor was referred to as power balance.

Privacy by design

Are the choices presented fairly and equally? This means giving people clear, understandable information about what the options mean for them and what each one involves (see below). Consent for personalised ads is unlikely to be freely given when people do not understand how their personal information is being used or that they can access the service without having to agree to the use of their personal information.

Respondents to the call for views were able to submit their feedback through two primary methods:

- Providing an **email response** allowing participants to provide unstructured feedback and submit attachments; or
- Answering a '**Smart Survey'** consisted of 29 questions with a combination of Likert scale questions[2] and open text responses across each of the four factors.

Overall, we received and analysed more than 2,280 email responses and 166 Smart Survey responses.[3] We have considered respondents' views carefully. This feedback has offered valuable insights into current stakeholder sentiments about and understanding of "consent or pay" models; and provided suggestions about approaches to regulation. We have considered respondents' views carefully and used them to inform our guidance on "consent or pay".

1.3. Summary of survey responses

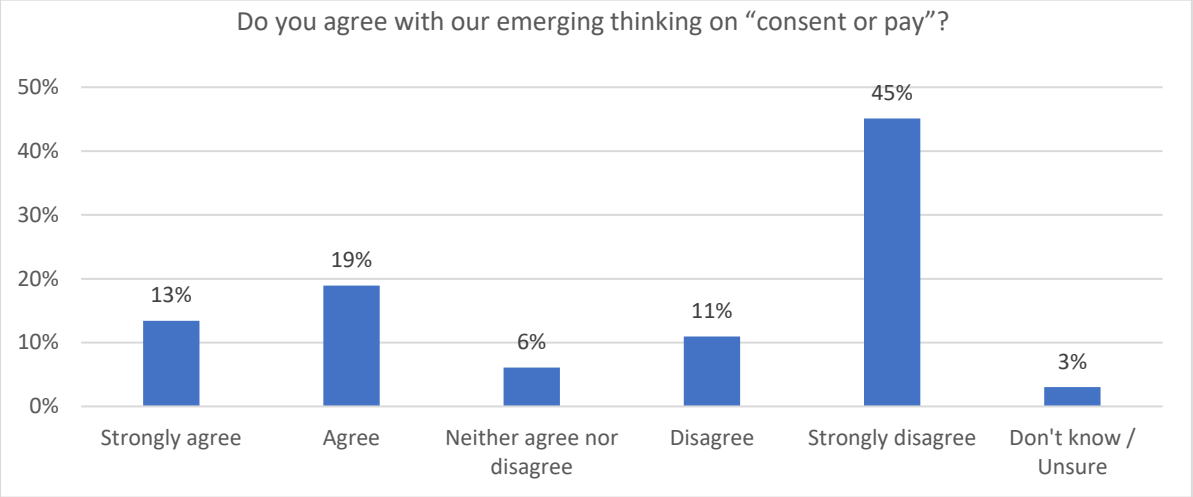
Our Smart Survey included several questions that aimed to capture respondents' overall levels of confidence and agreement with the factors set out in the call for views, and whether they found our emerging thinking helpful.

We asked respondents about whether they agreed with our emerging thinking on "consent or pay" models (set out in Figure 1 below). Many respondents reported disagreeing (11%) or strongly disagreeing (45%) with our emerging thinking. We also asked how helpful each of the factors are in comprehensively assessing whether "consent or pay" models comply with data protection law. Despite the majority indicating that they

[2] A Likert scale is a psychometric response scale to obtain a respondents' views or degree of agreement with statements. Respondents were asked to respond on a five-point scale.
[3] 2,250 of the email responses were received from individuals responding as part of an initiative organised by a campaign group named Ekō (Ekō - Menschen und Planet vor Profit).

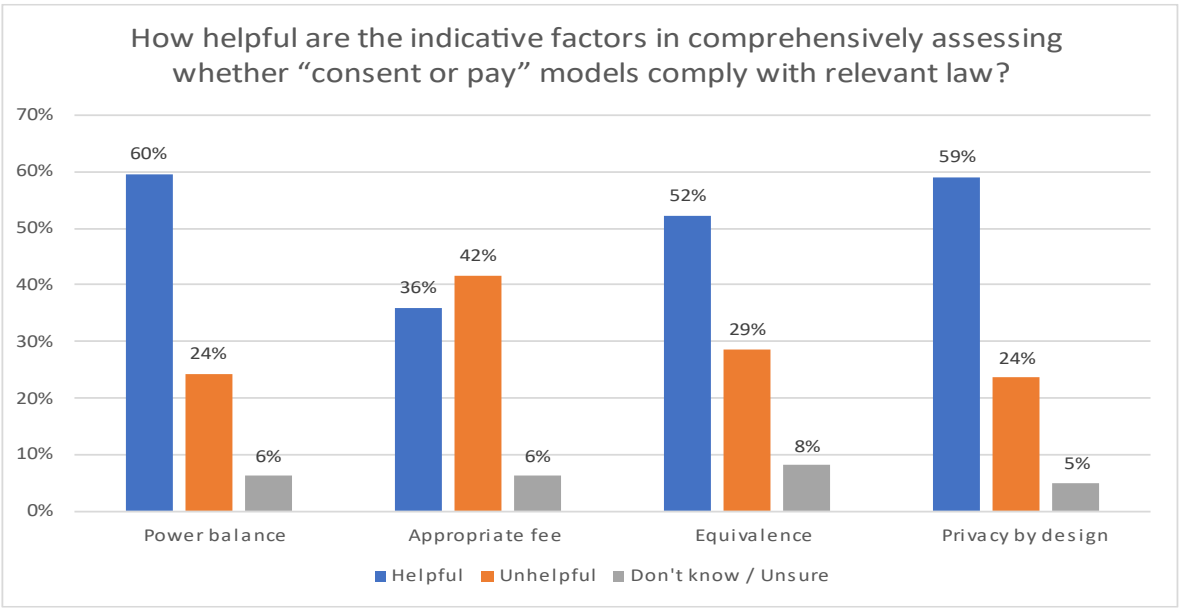
disagreed with our emerging thinking about "consent or pay" (as set out in Figure 1), the responses presented in Figure 2 show that the clear majority of respondents felt that most of the factors were helpful for assessing whether such models comply with the law.

Figure 1: Agreement with emerging thinking set out in the call for views



Source: ICO Consent or pay Smart Survey, sample 166 respondents.

Figure 2: Respondents view of whether ICO factors were helpful in assessing whether consent or pay models comply with the law4



Source: ICO Consent or pay Smart Survey, sample 166 respondents.

Most respondents reported power imbalance, equivalence and privacy by design as helpful. For power imbalance, 60% reported the factor as helpful

[4] Responses were classified as "helpful" if respondents reported the factors as "helpful" or "very helpful". Responses were classified as "unhelpful" if respondents reported the as "unhelpful" or "very unhelpful".

whilst just 24% reported it as unhelpful. Similarly, respondents rated privacy by design highly, with 59% reporting the factor as helpful and 24% reporting it as unhelpful. 52% reported equivalence as a helpful factor, with 29% reporting the factor as unhelpful.

Amongst the four factors set out in the call for views, respondents ranked "appropriate fee" as the least helpful, with only 36% reporting the factor as helpful. The responses to appropriate fee, evidenced by respondents' comments, mostly reflected disagreement from the public and campaign groups that organisations should charge any fee; and disagreement from organisations that their services should be subject to price regulation.

The remainder of this document summarises the main points and recommendations from the consultation responses across each of the four factors set out in our call for views. We provide a brief response to the key themes and explain, where relevant, how we have taken these into account in our "consent or pay" guidance.

This summary is not intended to be a comprehensive record of all the views expressed, nor to be a comprehensive response to all individual points raised by respondents. A full list of respondents via email is provided, along with redacted versions of their responses.

2. Power imbalance

The inclusion of "power imbalance" was seen as the most helpful principle outlined by the ICO in its call, with 60% of survey respondents highlighting the factor as "helpful". The comments have been summarised into the following key themes:

- **Lack of choice:**

  Several respondents expressed the view that an imbalance of power could make it challenging for organisations to implement consent or pay models in a compliant way. These respondents noted that consent under consent or pay models is not freely given if people lack a meaningful choice or if access to the product or service is conditional on the consent for processing, despite that processing not being necessary for the service.

- **Assessing the nature of the service:**

  Many respondents considered that the nature of the service would need to be assessed to understand whether consent or pay models could be implemented in a compliant manner. Respondents expressed views that organisations that provide "essential" services should not adopt consent or pay models as this would remove the possibility for consumers to leave the service.

- **Market power:**

  Respondents, particularly individuals responding in a private capacity, noted views that certain sectors considering the implementation of consent or pay models have players with significant "market power", affecting consumer choice and the ability to leave the service. Other respondents expressed views that market power should not be determinative as to whether a consent or pay model can be compliant under data protection law, as market power does not preclude an organisation from being able to validly obtain consent from their users.

- **The ICO's ability to assess power imbalance:**

  Some respondents highlighted that terms such as "market power" do not exist within data protection law and are therefore outside of the ICO's remit to regulate.

We have taken these comments into account in developing our thinking on power imbalance and taken the following actions when producing our guidance.

In our guidance we:

- Explain how power imbalance is relevant for organisations using or considering using consent or pay models for demonstrating that people can freely give consent.
- Provide a range of factors that can cause a power imbalance which organisations should consider as part of their assessment, including different groups of people that use or may use the service (such as those in a vulnerable position or where the service is intended for children), the impact on existing users of the service and the organisation's position in the market.
- Set out how an organisation's position in the market could feed into its assessment of power imbalance to understand whether consent has been freely given under consent or pay models.
- Set out steps for organisations to address a power imbalance.

A more detailed summary and response to the key themes raised in the call for views are set out in the following subsections.

2.1. Lack of choice

Several respondents referred to article 7[5] and recital 42[6] UK GDPR and European Data Protection Board (EDPB) opinion 08/2024[7] to highlight views

[5] UK GDPR article 7 sets out the conditions for consent: *"(1) Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data. (2) If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding. (3) The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent. (4) When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."*

[6] UK GDPR recital 42 states: *"Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment."*

[7] European Data Protection Board, Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms

that consent under consent or pay models is not freely given if people lack a meaningful choice. Respondents noted that under recital 42, consent should not be regarded as freely given if people are unable to refuse consent without detriment". Respondents pointed out that if refusal of consent can only take place either by paying a fee or by leaving the service, there is clear detriment to users. Some respondents also highlighted that such a detriment could be more pronounced for existing users, who may be more reliant on the service.

Several respondents referred to recital 43[8] and ICO guidance that says consent to processing should not be a condition of accessing a product or service unless that processing is necessary for the service. Many referred to the idea that processing for personalised advertising is not necessary for the provision of the core product or service and therefore access to the product or service should not be conditional on the acceptance of personalised advertising. These respondents expressed that consent or pay models are not providing people with a meaningful choice to refuse the processing of personal data for non-essential purposes.

Other respondents provided counterarguments, expressing the view that offering a "pay" option allows people to access the service without accepting the processing of data for non-essential purposes, thereby removing the conditionality.

ICO response

The UK GDPR sets a high standard for consent to ensure that people are being offered real choice and control over their personal data. Consent or pay models can only be compliant with UK data protection law where an organisation can demonstrate that people can freely give their consent under UK GDPR. Our "consent or pay" guidance sets out several factors that organisations should consider when demonstrating that people can freely give their consent.

The UK GDPR is clear that consent should not be bundled up as a condition of service unless it is necessary for that service. As a result, if people can

[8] UK GDPR recital 43 states: "*In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.*"

only access a product or service by consenting to processing for personalised advertising, this creates a situation of conditionality meaning consent is unlikely to be valid. Offering a "pay" option can provide people with an additional way to access the service without giving their consent to personalised advertising and provide more choice for people. However, if people who rely on the service are "priced out" of the "pay" option, they may have no realistic choice other than to consent and it may be more challenging for organisations to demonstrate freely given consent. Our guidance sets out these considerations to help organisations assess how and whether consent can be freely given.

In line with many of the call for view responses and recital 42, our "consent or pay" guidance sets out that consent is unlikely to be freely given if people do not have a realistic choice about whether to consent to personalised advertising to access a product or service. Our guidance sets out that if people are reliant on the service or may be unfairly penalised if they can no longer access the product or service, consent is unlikely to be freely given.

Our guidance sets out that if organisations have a clear power imbalance with the people who use their product or service, they could still rely on consent for personalised advertising, but it will be more difficult to demonstrate that consent has been freely given. By following the guidance, organisations should demonstrate how their model provides people with genuine choice around their data use.

2.2. Assessing the nature of the service

The call for views responses illustrated concern that websites and applications required for things like work, research, or broader public services could adopt "consent or pay" models, for example for pharmaceutical services, paying bills, recruitment etc. Respondents highlighted the potential for detriment to users if these products and services were to all require a fee to avoid the processing of personal data for advertising.

Many respondents suggested that whether the use of a consent or pay model complies with data protection law should require a case-by-case assessment considering the nature and necessity of the service. Respondents pointed to recital 43 of the UK GDPR which explains that consent should not provide a valid lawful basis for the processing of personal data "where there is a clear power imbalance between the data subject and the controller". The recital sets out that certain kinds of

controllers such as a public authority may have a clear power imbalance with data subjects and therefore mean that it is unlikely consent will be freely given.

Some respondents expressed the view that a distinction should be considered in relation to essential services when assessing whether consent has been freely given. They highlighted that where people rely on the service and have no genuine choice but to use a specific organisation, consent cannot be deemed freely given under a consent or pay model. For example, respondents noted that public services or utility companies should not be allowed to implement consent or pay models as people are unable to leave the service for an alternative provider.

Some respondents expressed views that social media is an essential service to connect and communicate with others, citing the EDPB's opinion on consent or pay in the context of large online platforms which sets out that a detriment may occur when certain social media services are "decisive for the data subjects' participation in social life"[9]; or it becomes impossible for them to refuse or withdraw consent from a service "that is part of their daily lives and has a prominent role"[10] without detriment. Other respondents considered social media as purely optional activities with many people navigating life without them and noted that providers of non-essential services ought to have the freedom to charge a fee for their services.

ICO response

Our guidance addresses these concerns in our proposed assessment of power imbalance. It highlights that consent for processing personal data is unlikely to be freely given when people have little or no choice about whether to use a service or not. The UK GDPR does not define categories of services as essential and it would be inappropriate for the ICO to adopt guidance that took such an approach. Our guidance sets out that organisations should consider the extent to which people rely on their products or services, and whether people will suffer detriment if they refuse or withdraw consent.

We highlight that where there is a clear power imbalance between an organisation and the people that use the product or service, it will be more difficult for organisations to demonstrate that consent can be freely given.

[9] European Data Protection Board, Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms, para 88.
[10] European Data Protection Board, Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms, EDPB opinion at para 87.

Recital 43 of the UK GDPR and our consent guidance gives the example of where the organisation is a public authority or an employer in an employer to employee relationship.

Our consent or pay guidance sets out our expectations for how organisations should assess power imbalance to demonstrate that people can freely give consent. It provides a range of factors that organisations should consider as part of their assessment of power imbalance, including different groups of people that use or may use the service (such as those in a vulnerable position or where the service is intended for children), the impact on existing users of the service, and the organisation's position in the market. Organisations should be able to demonstrate that there is no detriment to a person for refusing consent.

2.3. Market power

Many respondents observed that some sectors considering the implementation of consent or pay models contain organisations with large market shares. Respondents explained that where a small number of organisations hold market power, the implementation of consent or pay models could be unfair, at the expense of the rights of individuals.

Other respondents explained that the presence of market power would not preclude an organisation from being able to validly obtain consent from their users. The Court of Justice of the European Union's ruling in *Meta Platforms v Bundeskartellamt* was cited as an example of where market dominance does not automatically make consent invalid.[11] Respondents also suggested that there cannot be different standards of data protection compliance placed on organisations depending on their size or market position.

Other respondents, particularly publishers, expressed the view that the news market had more nuanced power dynamics in comparison to large social media platforms. News media publishers submitted that the ecosystem in which they operate is highly competitive and consumers have significant power as they can opt for alternative news publishers, including the BBC, which is funded by licence fees and does not rely on personalised advertising.

ICO response

[11] Judgment of the Court of Justice of the European Union, July 2023, Meta Platforms v Bundeskartellamt

Under consent or pay mechanisms, considering the power imbalance between organisations and the people that use the product or service is important to ensure that people can freely give consent. Our guidance sets out several factors that can cause a power imbalance. This includes where an organisation has a dominant position under competition law, which could be a relevant consideration in assessing whether it causes a power imbalance under data protection law and affects whether people can freely give their consent. This is because an organisation's market position may affect people's freedom of choice if they do not have realistic alternative options available to them other than to use that provider's product or service. This can result in detriment if people refuse or withdraw consent and can make it more challenging for organisations to demonstrate that people are able to freely give consent.

However, we agree with respondents' views that the presence of market power should not be the sole indicator of power imbalance, and that the presence of market power does not automatically preclude organisations from being able to validly obtain consent from their users. Where a power imbalance exists, organisations may still be able to rely on consent for processing, but it is likely to be more difficult to demonstrate that consent is freely given. Our guidance emphasises that this is a holistic assessment. No single factor can determine whether a "consent or pay" model has met the requirements for valid consent.

Where there is a clear power imbalance, our guidance sets out that organisations should take steps to address the imbalance to ensure people can freely give their consent. For example, organisations could do this by offering an alternative way to access their service that doesn't rely on the user consenting to personalised advertising or paying to avoid personalised advertising, or by introducing effective ways for people to transfer their personal data to another provider that offers a similar product or service.

2.4. The ICO's ability to assess "market power"

Some respondents highlighted that the definition of "market power" does not exist within data protection law and fall within the sphere of UK competition law. Therefore, any assessment of dominance or market power should consider principles developed under competition law and involve the UK's Competition and Markets Authority (CMA). Respondents suggested there was a risk that the ICO could be operating in areas outside of its competence if assessments of market power are carried out by the ICO when it is evaluating compliance with data protection laws.

ICO response

In the context of understanding whether consent has been freely given, the UK GDPR states that consent is not valid if there is a "clear imbalance of power" between an organisation and the person whose data they are processing.

Our "consent or pay" guidance sets out that organisations are responsible for demonstrating that consent has been freely given, including assessing whether there is a clear power imbalance with users. It explains that a clear power imbalance can arise from a variety of factors, including the nature of the service an organisation provides, the extent to which people rely on its service, and its position in the market. An organisation's position in the market is a relevant consideration in assessing whether people can freely give their consent, as people might be unable to refuse or withdraw consent without detriment.

In line with the comments received, our guidance clarifies that the ICO does not propose to define or assess market power. This is a matter for the CMA, other regulators with competition law powers or for the courts.

Our concern relates to whether an organisation's position in the market creates a power imbalance with users. Organisations should consider if their position in the market affects whether people can freely give their consent under a "consent or pay" model. We explain that the CMA's guidance on the digital markets competition regime (external link) may aid organisations when assessing whether there is likely to be a power imbalance arising from their market position. Where necessary, we will cooperate with the CMA and seek their views on questions of market power where this is relevant to assessing power imbalance under data protection law.

Recognising the importance of regulatory certainty and coherence, we have consulted with the CMA on the development of our guidance.

3. Appropriate fee

The principle of "appropriate fee" was reported as the least "helpful" amongst the four factors set out in the ICO's call for views, with 36% of survey respondents highlighting the factor as "helpful". The comments provided about the factor have been summarised into the following key themes:

- **The impact of a fee on freely given consent**:

  Many respondents, particularly individuals responding in a private capacity, expressed frustration and disagreement that consent could be freely given if any fee were introduced in consent or pay models. Respondents expressed the view that consent or pay business models do not meet the legislative requirements for freely given consent under the UK GDPR as any fee would result in a detriment to withdrawing consent.

- **Freedom to conduct business:**

  Many respondents, particularly organisations from the private sector, expressed concerns that the ICO's preliminary thinking on the "appropriate fee" implied price regulating their services. These respondents expressed that organisations should be free to choose business models and set prices to ensure financial viability. Other respondents proposed a variety of other funding mechanisms, including contextual advertising and subscription models, that are compliant with data protection law, that do not require a fee as an alternative to withdrawing consent.

- **Methodologies for setting an appropriate fee:**

  Respondents proposed several approaches for assessing an appropriate fee and many respondents had views on the suitability of the methodologies.

- **The ICO's ability to assess and set prices independently**:

  Respondents raised concerns around the ability for data protection authorities to set prices, highlighting the importance of collaboration with the CMA.

- **Social inequality:**

  Respondents highlighted that discussions on consent or pay must acknowledge the potential to exacerbate social inequality, discriminating against individuals from lower socio-economic backgrounds or in vulnerable situations. Respondents expressed

concern that privacy could become a right only for those who can afford it.

We have taken these comments into account in developing our thinking on appropriate fee and taken the following actions when producing our guidance.

In our guidance we:

- Provide clarity that the appropriate fee in the context of data protection law is relevant to assess whether people can freely give consent and does not relate to the value of the product or service being provided.
- Are clear that this is not a price-capping exercise, and that the onus should be on the organisation implementing a consent or pay model to demonstrate that people can freely give consent.
- Provide flexibility about how fees are calculated, acknowledging that an appropriate fee could depend on several factors that vary by provider.

A more detailed summary and response to the key themes raised in the call for views are set out in the following subsections.

3.1. Impact of a fee on freely given consent

Many respondents (particularly individuals acting in a private capacity) expressed views that introducing a fee in consent or pay models does not meet the legislative requirements for freely given consent. Many respondents referred to article 4(11)[12], article 7 and recital 42 of the UK GDPR, expressing the view that the presence of a fee or loss of access to the service does not allow people to refuse or withdraw consent without detriment.

Several respondents also referred to article 21(2)[13] highlighting the view that data subjects have the right to object to processing for direct marketing purposes free of charge.

[12] UK GDPR article 4(11) states: "'*consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*;"

[13] UK GDPR article 21(2) states: "*Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing*."

Respondents also noted the EDPB opinion under article 6(1)(a)[14] stating that personal data cannot be considered as a tradeable commodity.

ICO response

The UK GDPR sets out under recital 42 that people must be able to refuse or withdraw consent without detriment. Our consent or pay guidance sets out that offering a "pay" option as an alternative to consent does not automatically mean that consent is invalid. A fee does not necessarily result in an unfair penalty to a person. For example, our ICO consent guidance sets out that organisations may be able to incentivise consent, including with financial incentives.

However, organisations must be careful not to cross the line and unfairly penalise those who refuse consent. Our guidance explains that if the fee for the "pay" option is set too high, organisations may struggle to demonstrate that people can freely give their consent. This is because people may be priced out of the "pay" option and feel that they have no genuine or free choice but to consent to personalised advertising.

In addition, under article 21(2) of the UK GDPR, data subjects have the right to object to processing for direct marketing purposes. Under article 12(5) and recital 70, the provision of this right must be free of charge.[15]

Our guidance sets out that organisations must ensure that people can exercise the right to object to direct marketing, including online personalised advertising, free of charge. In practice the withdrawal of consent to personalised advertising will act as an objection to direct marketing.

3.2. Freedom to conduct business

Many private-sector respondents, particularly news publishers and advertising associations, reported that without moving to consent or pay models, their businesses would become financially unsustainable. Respondents highlighted recent interventions by the ICO relating to storage and access technologies, including the implementation of "Reject All"

[14] European Data Protection Board, Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms

[15] UK GDPR article 12(5) states: *"Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge."*

buttons, were already impacting the monetisation of their content, leading to significant revenue implications.

Respondents also expressed concerns that the ICO's initial thinking set out in the call for views would result in allowing people to access services for free; that is, without either direct payment or by way of using personalised advertising to generate revenue. These respondents highlighted that users do not have the right to access products and services for free and that data protection law should not prohibit organisations from charging for the use of their platform or imposing a fee to access content where none was previously payable. Respondents also expressed views that service providers should be able to set their own prices, as organisations have the right to freely conduct business.

Many respondents, particularly individuals acting in a private capacity, noted that organisations can continue to monetise their content through other funding models without charging a fee to refuse consent. Several respondents suggested that contextual advertising or subscription models could be used as alternative ways for organisations to charge for the provision of their products or services. Respondents proposed that in models reliant on advertising, consumers could be presented with a choice to either consent or reject tracking free of charge. If the consumer does not provide consent, then contextual advertising continues to be a way to monetise online content without the processing of personal data. Respondents also proposed additional "no-ad" tiers that could allow organisations to charge to remove all advertising from their services. These mechanisms could allow organisations to charge for their service, whilst also providing users with additional, free choice when it comes to consenting to the processing of personal data for the purpose of personalised advertising.

ICO response

The "appropriate fee" principle elicited diverging and opposed views, uncovering potential for misinterpretation of the factor. The ICO does not propose to regulate how much organisations charge for their products or services and does not propose that these organisations need to provide their services free of charge.

However, it is the ICO's role to ensure that the funding and business models selected by organisations are compliant with UK data protection law. We understand that a lot of the organisations considering the implementation of a consent or pay business model are reliant on funding through personalised advertising. However, using personalised advertising requires

the processing of personal data and therefore, requires a valid lawful basis for processing under the UK GDPR.

Where organisations are relying on consent as a lawful basis for processing people's personal data, they must be able to demonstrate that people can freely give their consent. Our guidance explains that an "appropriate fee" in the context of "consent or pay" models and from a data protection perspective, therefore refers to an amount at which people can freely give their consent. The level of fee for the "pay" option is a relevant consideration because if the fee is set at too high a level, people may be priced out of the "pay" option and it may make people feel they have no genuine or free choice but to give consent to personalised advertising.

In line with respondents' views, our guidance on appropriate fee does not prevent organisations from adopting a variety of other business models and pricing structures that are compliant with data protection law to charge for their products and services. For example, organisations can adopt different tiered subscription options in addition to the "consent" or "pay" options or could use other models, such as contextual advertising, to monetise their products.

It is for organisations to decide how they want to monetise their products or services. However, if an organisation chooses a "consent or pay" model they must be able to demonstrate that people can freely give their consent in line with data protection law. The factors in our guidance provide a framework for that assessment.

3.3. Methodologies for setting an appropriate fee

Three basic approaches for setting an appropriate fee in the context of consent or pay models were proposed in the call for view responses: revenues, costs, and consumers' willingness to pay. We summarise the proposals and our considerations for each of these methodologies below.

Using revenue to set an appropriate fee

Many respondents proposed that the fee within a consent or pay model should be set to allow organisations to recover any lost revenue from the inability to monetise their content through personalised advertising. These respondents proposed to use measures such as average revenue per user (ARPU) to determine an "appropriate fee". Such pricing models could allow organisations to continue to achieve the same revenue. Many highlighted that this would be important for the financial sustainability of their

organisations, with many stating that the implementation of "Reject All" buttons had already negatively impacted the monetisation of their content.

However, some respondents also highlighted challenges with using ARPU as an appropriate measure for assessing an "appropriate fee":

- Respondents noted challenges around tracking users across sessions and devices, where one person may be counted as two different users by measurement companies, reducing measures like the ARPU. As a result, these respondents noted that organisations should be allowed to set a fee higher than the ARPU for the revenues to remain unchanged.
- Respondents noted that advertising returns vary significantly between users. Respondents proposed that users with a higher-than-average ARPU would be more likely to opt for the "pay" option as those who value privacy more or those who consume more content are most likely to benefit from the "pay" option. Similarly, wealthier, less price-sensitive users, who are more likely to pay to remove advertising, are also likely worth more to advertisers. Respondents suggested that the fee would therefore need to account for this disproportionate lost advertising revenue from high-content users.
- Other respondents also expressed views that many of the large digital platforms considering consent or pay models have "significant market power" with an ability to influence prices in the market, making ARPU an unsuitable measure.

Some respondents, including data rights activists, reported that pricing in existing consent or pay models is "in considerable excess" of ARPU. They submitted evidence that suggested paying accounts make up less than 0.1% of existing consent or pay website users, stating that the consent or pay model is therefore not a reliable source of income, but is being used as a tool to increase consent rates.

ICO response

In the context of data protection law, an appropriate fee refers to an amount at which people can freely give their consent. Whilst in principle setting the fee to generate the same overall revenue can leave the organisation in an unchanged financial position, our guidance sets out that this measure is unlikely to be useful to understand whether a fee is appropriate in a data protection context.

Revenues, even when expressed on a per user basis, reflect the value of advertising to organisations on one side of a two-sided market, and not the

value that consumers associate with paying to avoid personalised advertising. It is therefore not representative of the value relating to an "appropriate fee" in the context of consent – that is, a fee that means people have a meaningful choice between consent or pay.

In addition, one of the central concerns raised by respondents about consent or pay models is the presence of a power imbalance between organisations and their users. Where there is a clear power imbalance with its users, an organisation may have the ability and incentive to set the price for the "pay" option above the level that would be expected where users did not face such an imbalance of power and had a realistic alternative.

Using costs to set an appropriate fee

Other respondents proposed cost modelling to establish an appropriate fee, as is often performed by utility regulators. However, other respondents noted that the cost structures vary significantly across the types of organisations considering the implementation of consent or pay models, with content being licensed, created or user generated. In addition, respondents noted that the information required for such a cost assessment is highly confidential and commercially sensitive.

ICO response

Regulatory interventions in relation to prices, such as those in regulated utilities, often rely on modelling of costs. However, it isn't the ICO's role to assess costs or set prices regarding organisations' products and services. These are commercial decisions for organisations to take.

In the context of consent or pay, the assessment of an appropriate fee relates to an amount at which people can freely give their consent. As a result, an assessment of the organisation's costs is unlikely to be an appropriate measure for this value.

Using consumer valuations to set an appropriate fee

The third approach to setting and assessing an appropriate fee is the idea of consumer valuations.

Some respondents suggested benchmarking pricing across different subscription models to assess people's willingness to pay for different services. Other respondents suggested that setting a price based on consumer's willingness to pay for the service created an assumption that consumers are entitled to access services for a price that they like.

Other respondents noted that the appropriate fee should relate to the value which people would be willing to accept or pay in return for sharing personal data for the purposes of personalised advertising. However, respondents noted that due to the highly unique and contextual nature of evaluations, this is hard to quantify.

ICO response

In the context of "consent or pay" models and from a data protection perspective, an appropriate fee refers to an amount at which people can freely give their consent to the processing of their personal data for personalised advertising. An "appropriate fee" should therefore reflect the fee that consumers attribute to the avoidance of their data being processed for the purposes of personalised advertising.

It is important to distinguish between this appropriate fee and the valuation that people might place on the core service. Whilst the value that people place on the core service is relevant to firms' pricing decisions around that core service, it will not reflect the fee that consumers attribute to the avoidance of their data being processed for the purposes of personalised advertising. Where a single price covers both these aspects it may be difficult to demonstrate that there is an appropriate fee.

Benchmarking against other services is also likely to be challenging as a means to demonstrate an appropriate fee, particularly where the comparators involve different core services, and the market circumstances may vary or are specific to the organisation operating the service.

Our guidance explains that the most appropriate measure of whether the level of fee can enable freely given consent is the value that people that use or could use the product or service associate with not sharing their personal information for the purposes of personalised advertising. We set out that using consumer valuations specific to this question are the most appropriate for setting or assessing an appropriate fee.

However, we note that estimating these values involves some complexities, as flagged by respondents in the call for views. Our guidance provides several factors that organisations could consider when assessing whether their fee is appropriate in the context of consent, including consumer research, consideration of income levels and monitoring of people's choices.

3.4. The ICO's ability to set prices

Several respondents raised concerns about the ability and jurisdiction for data protection authorities to conduct the analysis necessary for assessing an appropriate fee.[16] For example, several respondents noted that this needs to be done in conjunction with competition and consumer protection agencies due to the confidential commercial and financial information required for assessing a reasonable price.

Other respondents noted that determining an appropriate price should not be up to the ICO, but that organisations should be required to demonstrate that consent has been freely given at the selected fee.

ICO response

It is not the ICO's role to assess or set prices or pricing structures regarding organisations' products and services. In the context of consent or pay, the assessment of an appropriate fee relates to a fee at which people can freely give consent. As a result, consideration of the "appropriate fee" factor does not consist of data protection authorities setting prices or regulating how much organisations charge for their products or services.

Acknowledging that the fee at which people can freely give consent will depend on several factors that vary between providers, our guidance provides flexibility and does not prescribe an appropriate price or a range of appropriate prices. In keeping with article 7(1) UK GDPR and the accountability principle in article 5(2) UK GDPR, it is for organisations to demonstrate that people can freely give consent within their consent or pay models.[17]

3.5. Social inequality

Another theme expressed by respondents in the call for views was the idea that privacy should be a right for everyone and not just for those who can afford it.

Several respondents, particularly individuals and consumer rights organisations, highlighted that consent or pay models could exacerbate existing social inequality. For example, respondents commented that

[16] These concerns also relate to assessments of competition, which are relevant to the consideration of 'power balance' as another factor identified in the call for views.
[17] UK GDPR article 5(2) states: *"The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."*

individuals without access to their own financial accounts (for example, due to either financial hardship or abusive relationships) would be unable to select the "pay" option. Similarly, respondents suggested that a fee could discriminate against "less informed" users that are unaware of the value of their personal data or how their personal data is being used.

There were a significant number of responses that referred to the heightened protections that exist for children under UK GDPR. Respondents highlighted that children are unable to legally consent and are unlikely to have access to funds required to select the "pay" option. Points were also raised about children's lack of understanding of lengthy and legalistic terms and conditions and the risks of presenting children with consent or pay models as a result.

Respondents also highlighted the need to consider the development of consent or pay models in the market holistically, as opposed to only assessing the relationship between one organisation and its user. This is because if consent or pay models extended to multiple applications and services an individual uses in their daily life, the cost of multiple fees could become a significant barrier to privacy or access to services. For example, many respondents pointed to research by Noyb on consent or pay models, which estimates that if all companies followed similar pricing structures to those models launched in Europe, an individual would pay €251.88 per year.[18] Respondents also noted that Noyb's research suggests that a European family of four, with an average of 35 apps on their phones, "would face an annual bill of approximately €35,000 per year". Respondents therefore expressed views that many users could be "priced out" of the consent decision and that a "fair fee" would be dependent on social classes, income levels and specific individual context.

ICO response

Organisations are not obligated to provide their services free of charge. However, it is the ICO's role to ensure that the funding and business models selected by organisations are compliant with UK data protection law. Our guidance sets out that if the fee for the "pay" option is set too high, organisations may struggle to demonstrate that people can freely give their consent. This is because people may be priced out of the "pay" option and feel that they have no genuine or free choice but to consent to personalised advertising.

Our guidance also provides special consideration for children. Children are

[18] Noyb (2023), *noyb files GDPR complaint against Meta over "Pay or Okay"*

a vulnerable group and may lack financial independence or have a more limited understanding of what different processing activities mean for them. This may make it more challenging to demonstrate that they can freely give consent under consent or pay models. In line with article 8 UK GDPR, organisations must obtain parental consent for children under 13 and will need to implement effective age-assurance measures and make reasonable efforts to verify parental responsibility for those under the relevant age.[19]

In line with article 7(2), our position on privacy-by-design sets out that organisations should present requests for consent in an intelligible and easily accessible form, using clear and plain language. This will promote informed and accessible choices for all users of the service.

[19] UK GDPR article 8 states: *"[…] the processing of the personal data of a child shall be lawful where the child is at least 13 years old. Where the child is below the age of 13 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology."*

4. Equivalence

Respondents were supportive of equivalence as a principle for assessing consent or pay models, with 52% of survey respondents highlighting the factor as "helpful". The comments have been summarised into the following key themes:

- **Impact on service quality:**

  Respondents highlighted that the "consent" and "pay" options should provide people with the same service quality. Respondents expressed concerns that organisations could erode the quality of either the "pay" or "consent" models in such a way to nudge people to select one option over the other.

- **Bundling consent for personalised advertisements with premium services:**

  Many respondents referred to existing consent or pay models where the "pay" option included additional features or premium content. Some respondents agreed with the ICO's initial views that these models would not meet the requirements of equivalence, whilst others argued that including extra features in the "pay" option would not impact on freely given consent.

- **Need for increased clarity and links to other factors:**

  Some respondents acknowledged that equivalence is a relevant factor to be considered in the assessment of consent or pay models, but felt more clarity was needed from the ICO, particularly around how this factor relates to the requirement of freely given consent under the UK GDPR and how it works alongside the other data protection principles.

We have taken these comments into account in developing our thinking on equivalence and taken the following actions when producing our guidance.

In our guidance we:

- Set out that equivalence relates to offering broadly the same core product or service under the "consent" option and the "pay" option.
- Explain how the equivalence factor relates to freely given consent, namely that if the options offered are not equivalent, people may not have a genuine free choice to consent or not.

- Provide clarity about how incentives and bundling of additional features feed into the assessment of equivalence and freely given consent.
- Provide case studies setting out example assessments that consider all the factors set out in the call for views to help organisations understand how the principles should be considered in the round.

A more detailed summary and response to the key themes raised in the call for views are set out in the following subsections.

4.1. Impacts on service quality

Several respondents raised concerns regarding potential negative impacts on the overall quality of the service within consent or pay models.

Respondents expressed concern that organisations could erode the quality of the "consent" option to increase the uptake of the "pay" option. For example, respondents noted that organisations could gradually increase the number of advertisements shown over time on the "consent" option to nudge more people onto the "pay" option to potentially increase the monetisation of their services.

Other respondents highlighted that organisations could nudge people towards the "consent" option by providing poorer functionalities or incorrect rendering of content in the model without personalised advertising. Respondents noted that this could lead to more people selecting "consent" due to the poor service quality, rather than wanting to give consent.

ICO response

The UK GDPR is clear that consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment. Equivalence between the product or service offered under each of the "consent" and "pay" options is necessary to ensure that people have a genuine free choice over consenting to personalised advertising.

In line with the call for view responses highlighted above, our guidance sets out that failing to provide broadly the same core product or service under each option may lead to an unfair penalty. For example, if the "pay" option offers a lower-quality version of the core product or service or a completely different service altogether. This does not offer a genuine free choice, as people would effectively be forced to consent to personalised advertising to access the core service they are interested in.

Our guidance provides a list of non-exhaustive factors that organisations should consider in their assessment of equivalence. If there is a reduction of overall quality to the product or service for the "pay" option that amounts to an unfair penalty for refusing or withdrawing consent, organisations should ensure that this is a necessary and direct consequence of not processing personal data for personalised advertising purposes. Otherwise, the reduction in quality may amount to an unfair penalty, meaning that it's unlikely that any given consent would be valid.

4.2. Bundling consent for personalised advertisements with premium services

A number of respondents, particularly news media and advertising organisations, expressed views that data protection law should not prohibit organisations from being able to provide a free, ad-funded "consent" option and a "premium", ad-free service with additional features as the "pay" option, as long as the core service offered is the same. Respondents urged the ICO to consider the diverse range of funding models that publishers use, and to provide flexibility for organisations to freely conduct business.

Several respondents also queried why bundling additional features into a paid subscription model was problematic. The respondents explained that these additional features would make the paid-for option more attractive, thus reducing the pressure to consent.

Other respondents however expressed concerns that bundling different features could result in people having to pay more for the "pay" option than the equivalent monetary value of not accepting personalised advertising or could result in people making decisions based on the additional features provided within each option rather than their privacy preferences. These respondents were more supportive of the ICO's proposal to include equivalence as a factor for assessing whether people can freely give consent.

Some respondents suggested that the equivalence should only be relevant when there is a fee paid in lieu of personalised advertising, rather than when a fee related to "premium" subscriptions. For example, respondents drew the distinction between a subscription model with a basic and premium account and a consent or pay model, stating that the subject of equivalence should only be relevant to the latter business model.

ICO response

Our guidance on consent sets out that organisations can incentivise people to give consent in some circumstances, as long as this does not amount to an unfair penalty for those who do not consent. Organisations must be able to demonstrate that people can refuse consent without unfair penalty.

Our consent or pay guidance sets out that the core product or service organisations offer to users should be broadly the same under the "consent" and "pay" options. Organisations can offer features or benefits that are additional to the core service in the "consent" or "pay" options, as long as the core product or service is equivalent, of equivalent quality and the additional benefits or features do not change the nature of the core service.

Organisations should consider the effect of tying any additional non-core benefits to consent for personalised advertising as if there is a reduction of overall quality to the product or service for the "pay" option, then this may amount to an unfair penalty.

Our consent or pay guidance also outlines that organisations can include additional benefits in the "pay" option. However, organisations cannot use these benefits to set a higher, inappropriate fee for the "pay" option for avoiding the processing of personal data. Otherwise, it may lead to a price that is too high for those people who simply want to avoid the processing of their personal data. This could drive people to unwillingly select the "consent" option, making it more challenging for organisations to demonstrate that people can freely give consent (see appropriate fee section for more).

Our consent or pay guidance does not prevent organisations from charging for their product or service using a subscription model, contextual advertising models or other funding models. It also does not prevent organisations from offering further subscription options which provide additional features or benefits on top of their "consent" or "pay" options.

4.3. Need for increased clarity and links to other factors

Some respondents acknowledged that equivalence is a relevant factor to be considered in the assessment of consent of pay models, however they felt more clarity was needed from the ICO. In particular, respondents expressed uncertainty about how the equivalence factor relates to freely given consent under the UK GDPR, and how it would work alongside the other principles set out in the call for views.

ICO response

In our consent or pay guidance, we make clear why equivalence is relevant to consent or pay and link this to the requirements for freely given consent under the UK GDPR. We explain that equivalence between the product or service offered under each of the "consent" and "pay" options is necessary to ensure that people have a genuine free choice about consenting to personalised advertising. Throughout our guidance, we have provided additional information on how organisations could approach the assessment of their consent or pay models for each of the principles. We have also provided example case studies to help demonstrate how the factors work in the round.

5. Privacy by design

Respondents were supportive of privacy by design as a principle for assessing consent or pay models, with 59% of survey respondents highlighting the factor as "helpful". The comments have been summarised into the following key themes:

- **Online choice architecture**

  Many respondents noted that privacy by design should be a core principle that organisations factor into the design and choice architecture of their services. Many raised concerns over pre-selected options, overly complicated decisions and hidden changes to user terms nudging users into consenting. Respondents suggested that choice design within consent or pay would need to be specific, transparent and easy to understand for people to make informed choices.

- **Disempowerment and decision fatigue**

  Many responses highlighted that people are feeling disempowered when it comes to accessing online services. People reporting losing trust in how online services use their data and feeling disempowered about the level of control they have. Respondents raised concerns around existing decision fatigue that users experience around cookie-walls.

- **Sensitivity of data**

  Respondents raised concerns about people having to share their banking or payment details with online services where they do not want to consent to personalised advertising. Many respondents viewed their financial information as having a level of sensitivity and were concerned about the potential impact on them if this information was compromised.

- **Interactions with other technologies**

  Some responses offered suggestions on how consent or pay models can be implemented and the way these business models may interact with systems such as adblockers.

We have taken these comments into account in developing our thinking on privacy by design and have taken the following actions when producing our guidance.

In our guidance we:

- Ensure our position on privacy by design in relation to consent or pay models aligns with existing guidance on online choice architecture.
- Provide clear examples of fair and appropriate privacy by design principles.
- Provide clarity on the use and lawfulness of storage and access technologies.

A more detailed summary and response to the key themes raised in the call for views are set out in the following subsections.

5.1. Online choice architecture

Many respondents noted that privacy by design should be a core principle that organisations factor into the design and choice architecture of their services. Respondents agreed that organisations should provide users with clear and comprehensive information about the "consent" and "pay" options and that the design should enable users to exercise their information rights.

Respondents, particularly individuals, academics and civil society organisations, highlighted that many organisations still operate dark patterns designed to influence users to accept or consent to tracking. Respondents noted that many websites currently deploy deceptive design techniques including promoting unbalanced choices. Many highlighted that preventing the use of such harmful online choice architecture in the context of consent or pay models will be a key challenge for the ICO.

Many industry responses noted the considerable work in privacy by design that the ICO has already undertaken via the Children's Code[20] and work with the CMA on online choice architecture.[21] Many agreed that design choices that are deliberately intended to misinform or mislead end users should not be compliant. However, organisations also wanted the ICO to provide flexibility for organisations to decide what the right approach is for their service.

Some individuals responding in a private capacity noted that consent or pay may discriminate on the grounds of disabilities, referring to assistive

[20] Information Commissioner's Office, The Children's Code
[21] Digital Regulation Cooperation Forum, Harmful design in digital markets: How Online Choice Architecture practices can undermine consumer choice and control over personal information

technologies and the use of special browsers that are intended to work with screen readers. Respondents expressed concern that these technologies do not work with existing online choice architecture and that users with these particular needs may be forced to pay in order to make the product or service usable at all.

ICO response

When adopting a data protection by design approach, organisations have an obligation to find a design that works to achieve compliance across all data protection principles. Organisations must provide information to people in a way that is concise, transparent, intelligible, easily accessible and uses clear and plain language.

The ICO and CMA published a joint paper on harmful design in digital markets, focussing on how online choice architecture practices can undermine consumer choice and control over personal information.[22] Well-designed online choice architecture can guide users towards choices that align with their goals, preferences or best interests.

We consider that online choice architecture will be a key component to enable people to make informed decisions and freely give consent. Our guidance on consent or pay states that organisations must avoid using harmful design practices when presenting people with choices. Organisations must provide clear information about each of the options in the "consent or pay" model using concise, clear and plain language to enable people to make an informed decision. Our guidance also sets out best practice principles for how the "consent" and "pay" options should be designed and presented to be able to demonstrate people can freely give consent.

5.2. Disempowerment and decision fatigue

Many responses, particularly from individuals acting in a private capacity, expressed views that consent or pay models are "fundamentally unfair" or "wrong".

Many highlighted feeling disempowered over their choices regarding data and online privacy. Many respondents reported feeling that larger platforms

[22] Digital Regulation Cooperation Forum, Harmful design in digital markets: How Online Choice Architecture practices can undermine consumer choice and control over personal information

could force and coerce users into consent or pay models using dark patterns and tactics to encourage consent, leading to further lack of trust on the part of consumers. They highlighted the design choices often made by online services and how these contribute to issues of disempowerment and fatigue. For example, how many services allow them to consent with ease (one click) as opposed to requiring them to go through a more complex process to refuse (many clicks).

Respondents also expressed concern that the widespread use of consent or pay could increase the potential of fraudulent activities, for example through cloned or scam websites trying to access financial details. Respondents raised the need for users to understand what sits behind the paywall before deciding whether to consent or pay, to ensure that websites are not receiving payment or consent for the processing of personal data on unrelated, "clickbait" websites that do not provide value to the user. Respondents noted that the prominence of consent or pay models could increase the potential harms to less digitally literate or informed members of society.

Other respondents proposed a notion of imposing a "duty of care" for publishers of "do no harm".

ICO response

Literature related to data protection harms supports the idea that people's reported concerns about use of personal data and their actions and behaviours are often misaligned (sometimes termed the "privacy paradox").[23] This can be caused by several factors. For example, consumers may perceive the cost of trying to engage with understanding how personal data is collected, processed and shared, as greater than the perceived benefit of taking actions to protect their personal data. Similarly, consumers may be resigned to the fact that they have no alternative to using certain online services, to maintain social interactions and access specific markets. This results in consumers consenting to their personal data being collected and used, even if this contradicts their stated preferences.

It is important for the ICO to ensure consumers are making meaningful and informed decisions about their personal data. This includes tackling unwarranted nudging, information asymmetry and restriction of choice that can impact people's decision making. Genuine consent should put

[23] Information Commissioner's Office (2022), Overview of Data Protection Harms and the ICO's Taxonomy

individuals in charge, build trust and engagement, and enhance the reputation of organisations relying on it.

Our thinking on privacy by design in the context of consent or pay models aims to address harmful online choice architecture to ensure people are presented with choices in a fair, transparent and informed manner. The principles set out in our guidance intend to reduce the cost of engaging with privacy preferences and offer individuals real choice and control.

5.3. Sensitivity of data

Many responses expressed concerns about consent or pay being a means by which organisations could obtain more "first party data" about paying subscribers. Respondents highlighted that people may choose to create anonymised identities to access online services to avoid sharing personal data. Given that people would have to sign up to the online service and provide financial information to use the "pay" option, respondents noted that people could view this option as unviable due to risks of data breaches.

Those providing responses in an individual capacity also noted that this means both options inherently involve data processing and expressed concern that organisations in the private sector were not considering different ways of generating revenue. For example, respondents referred to contextual advertising and noted that a number of other effective advertising technology solutions exist that use less, or no personal data.

Others noted consent or pay focuses on behavioural advertising and does not address other forms of monitoring and tracking, which respondents suggested are often not necessary for service delivery.

ICO response

We agree with respondent's concerns of how personal data may be collected under the "pay" option. Our guidance includes a section on designing the "pay" option with privacy by design in mind. Organisations considering the implementation of consent or pay models should ensure the required compliance with all data protection principles when processing personal data under both the "consent" and "pay" option.

Due to the nature of the processing involved in personalised advertising, "consent or pay" models are likely to constitute high risk processing. Therefore, before organisations implement a "consent or pay" model, they must either review and update their existing Data Protection Impact Assessment (DPIA) covering the use of advertising technologies or conduct

a new one.

The "pay" option doesn't involve obtaining consent. However, organisations must build this option with privacy by design in mind from the outset.

5.4. Interactions with other technologies

Respondents expressed concern and curiosity about how consent or pay models interact with technologies like private browsing or adblockers. They said users could deploy these technologies to counter online tracking. For example, the possibility of users opening a private browsing window, clicking agree, and closing that window after their visit to minimise any tracking. However, they considered that it shouldn't be necessary for the user to "beat the system" in this way. Others asked how adblockers would be impacted.

ICO response

We agree that people should not have to deploy their own countermeasures, such as private browsing or adblockers, to achieve their preferred privacy setting. The ICO has undertaken considerable work in privacy by design to address harmful online choice architecture and to empower people to exercise their data protection rights in an informed and accessible way. We expect organisations considering the adoption of consent or pay mechanisms to consider and demonstrate they meet the requirements set out in our guidance.