Regulatory Sandbox Final Report: Meta Platforms, Inc

A summary of Meta Platforms, Inc's participation in the ICO's Regulatory Sandbox

Date: September 2025

Information Commissioner's Office

Contents

1. Introduction

1.1 The Regulatory Sandbox (Sandbox) is a service that the ICO provides to support organisations that are developing products or services which intend to use personal data in innovative and safe ways, and will deliver a potential public benefit.

1.2 The Sandbox is a free, professional service that is available to organisations of all sizes who meet our entry criteria and specified areas of focus. These criteria are assessed by the Sandbox's application processes. The ICO has published more information on the entry criteria in its guide to the Sandbox and the Sandbox's terms and conditions.

1.3 The Sandbox specifically seeks to engage with projects operating within challenging areas of data protection. Sandbox participants have the opportunity to engage with the ICO, draw upon its expertise and receive support on mitigating risks and implementing data protection by design and default into their product or service. This helps ensure that the participant identifies and implements appropriate protections and safeguards.

1.4 Meta Platforms, Inc (Meta) is a large, multinational technology company. It operates various social media platforms and communications services including Instagram and Facebook. Meta is a controller for UK data subjects in relation to its Instagram and Facebook services. Meta is currently researching a system, using certain privacy-enhancing technologies (PETs), which it states aims to enable the accurate measurement of the effectiveness of online advertising whilst protecting user privacy. Meta intends that the development, and potential deployment and adoption of this system will provide benefits for everyone that uses the internet, as well as the wider digital ecosystem. For the purposes of this report, the system will be referred to as Privacy Preserving Attribution (PPA). More detail on how PPA works is contained in section two of this report.

1.5 The ICO accepted Meta into the Sandbox in June 2024, determining that Meta's proposal aligned with the Sandbox's current areas of focus at the time of its application. Online tracking is a recent strategic priority for the ICO, which has included the development of its online tracking strategy.

1.6 The ICO and Meta agreed to work on the following objectives as part of Meta's bespoke Sandbox plan:

- **Objective one:** The ICO and Meta will work together to understand more about how Meta's PPA designs operate. This objective will help to provide initial information in relation to whether The Privacy and Electronic Communications Regulations 2003 (PECR) is in scope. It will also start to consider whether Meta's PPA designs will result in the processing of anonymous information.
- **Objective two:** The ICO, based on the information provided by Meta, will provide feedback on whether the use of PPA is likely to be captured within the scope of PECR.
- **Objective three:** The ICO and Meta will assess whether the information processed at the different stages of PPA should be treated as personal data and subject to the requirements of the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (DPA 2018). This objective will also consider whether any of the information can be considered to be anonymous and therefore outside of the scope of the UK GDPR.
- **Objective four:** The ICO and Meta will examine the balance between, and impacts on, privacy and utility in relation to Meta's proposed aggregation methods for the aggregated attribution reports produced by PPA. This objective will consider Meta's approach to using techniques such as differential privacy.
- **Objective five:** The ICO and Meta will discuss the governance model Meta is developing to provide safeguards to help ensure that parties within the helper party ecosystem respect restrictions on handling information (including any attempts to reidentify individuals).

1.7 Work commenced on the Sandbox plan in July 2024. The ICO and Meta concluded work on these objectives in April 2025. This report summarises the work that was carried out during Meta's time in the Sandbox.

1.8 With consultation from participating organisations, the Sandbox publishes exit reports for all participants so that fellow innovators facing similar questions about data protection by design and default can benefit from the key learnings and feedback from the Sandbox. It should be noted that the views in this report are based on the ICO's specific contextual understanding of Meta's operations and, therefore, it cannot be guaranteed that other

organisations will be able to apply these considerations in the same way. Considerations in this report are subject to change as the data protection landscape in the UK evolves and as Meta updates its practices.

2. Product description

2.1 Meta is currently researching and developing its approach to PPA. PPA is a system that performs online advertising attribution. Meta describes that its overarching purpose is to help organisations assess the effectiveness of online advertising campaigns. It does this by measuring the impact of online impressions (impressions), such as viewing or clicking on an advert, on online conversions (conversions), such as making a purchase. It then produces aggregated attribution reports for online advertisers (advertisers) and online advertising publishers (publishers). Meta suggests that PPA is one potential alternative to online advertising attribution approaches that use third-party cookies and similar technologies. However, Meta informed the ICO that the online tracking industry views that there are challenges which prevent this from being a commercially viable and scaled approach, hence exploring this through the Sandbox with the ICO.

2.2 Meta has included various PETs and technical safeguards within the technical design of PPA. These include:

- encryption;
- multiparty computation (MPC), engaging additional 'helper parties' to carry out the computations;
- secret sharing;
- differential privacy; and
- aggregation methods.

The ICO's MPC guidance identifies that secret sharing is a cryptographic technique. The guidance states that "This refers to the division of a secret and its distribution among each of the parties. This means that each participating

party's information is split into fragments to be shared with other parties."

2.3 During Sandbox participation, Meta presented different versions of its PPA designs to the Sandbox as they evolved. The following paragraphs of this section of the report detail a stage-by-stage overview of how PPA works, as described by Meta. That overview represents the most recent design that was considered within the Sandbox. The designs are technically and legally complex with areas that require further development, such as the governance framework, before specific processes are determined. This description is only intended to serve as an overview and not a detailed explanation of the designs, many aspects of which are still subject to consideration.

2.4 At 'Stage one' of the PPA process, a publisher will call a method, which is a request that can be made of an application programming interface (API), within the API when a person creates an impression by viewing or clicking on an online advert. This publisher will then transmit information to the device that person used to engage with the advert. Meta indicates that this information is required to allow subsequent conversions to be matched with relevant impressions.

2.5 At 'Stage two', the advertiser will call a separate API method when a conversion is created, such as a person purchasing a product or subscribing to a service. The advertiser will also transmit information to the person's device. This includes information to match conversions to impressions, a value associated to the conversion and other information used to construct the aggregated histogram report at the end of the process.

2.6 During 'Stage three', information is extracted from the person's device. The advertiser will then receive encrypted information (a histogram contribution) via the process outlined in Stage two. During Sandbox participation, Meta intended that the information will only relate to the last matching impression. Meta also stated that the information will only be received if the end user has not disabled the API, a conversion was matched to a saved impression, and the differential privacy protections have not been exhausted.

2.7 At 'Stage four', Meta describes that a batch of encrypted Stage three information is shared with the two organisations operating as helper parties. Those organisations are expected to be separate to the advertiser and publisher. Two helper parties will then perform the MPC function to analyse the contributions. When the information is received by

the helper parties, Meta states that the information will have been split into two 'secret shares' (which are essentially represented by randomised numbers) and each party can only decrypt one secret share. The information will then be aggregated together and have 'random noise' added via differential privacy methods. K-anonymity has been discussed within the World Wide Web Consortium (W3C) Private Advertising Technology Working Group with an intent to ensure that each 'bucket' within the histogram is sufficiently generalised to limit the likelihood of individuals in the output being directly or indirectly identifiable.

2.8 The final stage of the PPA design is 'Stage five'. Here, Meta indicates that the helper parties will return a 'differentially private histogram' to the advertiser. The advertisers can then use these aggregated attribution reports to assess how effective their online advertising is.

2.9 During the Sandbox project, Meta shared more detailed descriptions of the PPA designs with the ICO. It is publicly available via this W3C page. However, it should be noted that this page is subject to regular amendments and, as a result, may not be representative of the designs discussed during Sandbox participation.

3. Key data protection considerations

3.1 During Meta's participation in the Sandbox, the ICO and Meta considered key themes relevant to the development of PPA in relation to the objectives set out above. Those key themes are summarised below.

Does PECR apply?

3.2 In the UK, PECR is a law that sits alongside the UK GDPR and DPA 2018. It provides people with specific rights in relation to electronic communications. The ICO's interpretation of PECR, which is detailed in this report, is based on its understanding of PECR's requirements which were in force prior to the Data (Use and Access) Act 2025 (DUAA) coming into effect. Its rules related to the use of storage and access technologies are the most relevant to Meta's PPA designs. Specifically, regulation 6(1) of PECR states:

"Subject to paragraph (4), a person shall not use an electronic communications network to store information, or to gain access to information stored, in the terminal equipment of a subscriber or user unless the requirements of paragraph (2) are met."

Regulation 6 applies to anyone who stores information **or** gains access to information on a user's device. It does not only apply to cookies. It applies to any method of storing or accessing information on a user's device.

3.3 Paragraph 2 establishes further requirements for methods caught within the scope of regulation 6. It details the information that must be provided to people, and the obligation to gain their consent to use these methods. Regulation 6 does contain two exemptions to its requirements. However, their applicability is limited.

3.4 The ICO informed Meta that regulation 6 of PECR will apply to the use of PPA. However, it should be noted that that view applies to the designs reviewed at the time, and the requirements of PECR as they were in force during the Sandbox (ie wording in the legislation prior to the entry into force of the DUAA). This conclusion is explained in some further detail in the below sections.

3.5 Early in Meta's Sandbox participation, it described that for PPA to work, information would need to be stored on the user's device. In an earlier design of PPA, a 'one-time random ID' would be created on the user's device when the API is used. This would remain on the user's device for a short period of time until it is algorithmically converted into secret shares. The one-time random ID would then be removed from the user's device and the secret shares would be used to facilitate the online MPC element of PPA. The secret shares would remain on the user's device until they are used for online advertising attribution purposes. Therefore, the ICO concluded that regulation 6 of PECR would apply to this process as information would be stored and accessed on the user's device. The ICO also noted that PECR does not include an upper or lower time limit on what constitutes storage. Temporary storage still constitutes storage. Secret shares remain as an element of Meta's more recent designs.

3.6 Meta also indicated that PPA would need to store additional metadata in an on-device database. The ICO understands metadata to be basic information that describes the more detailed information it is connected to. In PPA's context this would include, but is not limited to, information such as:

- the app or website where an advert was shown to a person;
- the app or website that person navigated to;
- a timestamp of when an impression was created; and
- 'filter data' (used to determine the eligibility of an impression to receive attribution from a conversion) provided by the relevant app or website measuring attribution.

Meta intends that this metadata will be used to ensure that relevant online advert interactions can be assessed, and meaningful or useful online advertising attribution can take place. Therefore, the ICO concluded that storing this information on a person's device would be within scope of regulation 6 of PECR too.

3.7 At the end of the PPA process, an aggregated attribution report is produced. For those reports to provide useful and meaningful information for online advertising attribution, the statistics will be compiled based upon people's interactions with online advertising. That information is stored on the user's device. It is then extracted via the MPC process and included in the aggregated attribution reports that are produced. This further demonstrated to the ICO that throughout the PPA process, information will be both stored and accessed on the user's device, thus engaging regulation 6 of PECR.

3.8 The ICO was not of the view that regulation 6's exceptions would be engaged by the use of PPA. For example, the 'strictly necessary' exception applies where the use of storage or access technologies is essential to provide a service. However, the ICO views that strictly necessary must be considered from the view of the user, and not the provider of a service. The provision of advertising, or analysing its effectiveness, is not required by the user. As such, PPA will not be captured within this exception. The DUAA contains modifications to regulation 6's exceptions. It should be noted that DUAA changes were outside the scope of the Sandbox work and were not considered. However, the ICO has recently updated the above linked guidance and clarified that the new 'statistical purposes' and 'appearance' exceptions do not apply to online advertising purposes. It should be noted that the guidance on the new exemptions is currently in draft form.

3.9 While the ICO has determined that regulation 6 of PECR will apply to PPA, it should be noted that these requirements provide people with awareness and control over the information that is stored and accessed on their devices. The ICO acknowledges that Meta is researching methods to measure online advertising that aim to provide greater degrees of privacy for people. Developments in the AdTech and online tracking industries remain a focus for the ICO. The ICO welcomes Meta's work to explore how the adoption of PETs could be implemented to move towards less privacy intrusive approaches to measuring online advertising attribution where possible.

Does data protection law apply?

3.10 The UK GDPR and the DPA 2018 apply to the processing of personal data. Their requirements do not apply to the processing of anonymous information. Article 4(1) of the UK GDPR defines personal data as:

> "'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

3.11 The UK GDPR's Recital 26 helps to interpret the article 4 legal definition of personal data. It also states that people can be considered to be identifiable both directly and indirectly, and that account should be taken of all the means reasonably likely to be used, such as singling out, to identify someone. Recital 30 outlines how people can be associated with online identifiers, which can be used to help identify them.

3.12 The concept of identifiability is complex and was considered during Sandbox participation. The ICO used its draft anonymisation, pseudonymisation and PETs guidance to help inform its feedback to Meta. Since then, the ICO has published its finalised anonymisation guidance. The guidance explains that information is only effectively anonymous when the risk of someone being identified or identifiable is sufficiently remote. Organisations must assess the risk of information being identified or identifiable, and should consider the means reasonably likely to be used, on a context

specific basis. The ICO also used the key indicators of identifiability (ie singling out and linkability) to inform its feedback to Meta.

3.13 Based on the information provided, the ICO views that at Stages one to four of the PPA process, as described above, a risk of identifiability remains. Where that risk of identifiability is not sufficiently remote for the data to be considered anonymous, it will constitute the processing of personal data and data protection law will apply. The ICO expects Stages one to four to include the processing of personal data. This is explained further below. However, the ICO acknowledges that, if implemented appropriately, this proposal reduces data protection risks in comparison with existing industry practices, such as the use of third-party cookies. This could include security risks where pseudonymisation and encryption are used effectively. The ICO notes and is encouraged by the intention to deploy PETs to protect people's privacy, where they are used appropriately and effectively. Using PETs appropriately can also help organisations to comply with their data protection by design and default requirements. The ICO also views that the aggregated attribution reports (the Stage five output) may be effectively anonymous, depending on certain factors and how they are used. Some of those views are also outlined further below.

3.14 The ICO reiterates that any organisations that use PPA will remain responsible for conducting their own appropriate assessments of identifiability within their own unique contexts and use cases. Those assessments will need to assess the status of the information at each stage of the PPA process and in the hands of the different organisations involved. Information that is personal data to one organisation might be anonymous to another. However, the ICO's anonymisation guidance states that where a controller is processing personal data for a given purpose, this data will also be personal data in the hands of its joint controllers or processors processing it for the same purposes. Controller and processor relationships were not considered within the scope of the Sandbox.

3.15 The ICO informed Meta that it expects advertisers and publishers may possess significant amounts of personal data related to people whose information will be used within PPA. For example, advertisers might retain purchase or enquiry logs and publishers may hold account information and personal preferences. The ICO noted that the intention of PPA is not for those parties to combine various sources of information to identify people. However, organisations could misuse the information processed in Stages one to four of PPA, such as non-compliantly combining it with

personal data they already hold in an attempt to re-identify people. For example, it is possible to see how this may be advantageous to advertisers in use cases with high purchase values and smaller cohorts of customers. This could produce a risk of linkability between datasets.

3.16 Related to the above, the ICO views that advertisers having discretion over which histogram indexes (described further in section 3.17) are established in the Stage five output, and publishers assigning conversions to them, gives rise to a degree of risk of identifiability. It is possible that those organisations could misuse the process to repeatedly assign specific people, or small groups, to predefined histogram indexes in an attempt to identify them. The severity of this risk will depend on the context including:

- where organisations may collude with one another;
- the information relevant parties have available;
- the size of the groups in the histogram indexes; and
- the purposes for which any re-identified data may be used.

3.17 The ICO also suggested that there may be a risk of singling out. Singling out does not require the knowledge of someone's direct identifiers (such as their name). It just means that you can distinguish one individual from another, or isolate records that relate to a person within a dataset. At Stages one to four, PPA must be able to differentiate between the different contributions people make to produce a meaningful and useful Stage five output that advertisers can use. For example, it must be able to:

- understand that a person created an impression or conversion;
- understand when and where (such as the domain) an impression or conversion took place;
- match impressions with conversions for attribution; and
- assign a value to those events and understand which histogram index a person's activity relates to. Histogram

indexes are aggregated statistical sections within the Stage five output. They can be formed to represent different criteria such as a specific advert campaign, where an advert was shown, what was shown, when it was shown and to whom.

Therefore, PPA is required to differentiate one person's online activity from another's up until the point aggregation takes place.

3.18 Meta described to the ICO that the above information is contained within secret shares when it is sent to the MPC helper parties. The secret shares are essentially randomised numbers. Meta also stated that each helper party would receive one of two secret shares and the original values cannot be recovered unless they are combined. This is a positive data protection measure. The ICO believes that the secret sharing process would be an implementation of pseudonymisation where the UK GDPR's requirements for pseudonymisation are met. Pseudonymised personal data is still personal data and is within the scope of data protection law.

3.19 Article 4(5) of the UK GDPR states:

> "'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."

The ICO views that the secret sharing process, based on the information provided, meets this definition. For example, a secret share used in the computation and its underlying values can still be analysed and differentiated from others as part of the computation, even when each helper party only has access to an incomplete part of the information. That secret share may not be able to be attributed to a specific data subject without the use of the other secret shares used in the same computation. Where secret sharing within an MPC process is used effectively, the secret shares must be kept separately. Meta also states that technical and organisational measures (eg contractual stipulations) will be in place to prevent collusion.

3.20 The ICO acknowledges that Meta includes encryption at various stages of the PPA design. The UK GDPR identifies encryption as an appropriate technical security measure. The ICO has recently published updated encryption guidance which is linked to earlier in this report. Within it, it addresses where encrypted data is still personal data.

3.21 As detailed earlier in this section, the ICO informed Meta that the Stage five output of PPA could be effectively anonymous. This view is subject to various factors which may change for different use cases of PPA. This will also depend on who implements it and how they implement it. Some of those factors are listed below:

- The output is used solely as aggregated statistics to measure conversions in an online advertising campaign and not for any other purpose.
- K-anonymity and differential privacy are appropriately and robustly applied, and verified through appropriate testing (eg applying a motivated intruder test). This includes aspects such as an appropriate value of 'K' and 'epsilon' to prevent singling out and linkability attacks. It also includes minimum cohort sizes and a wide enough in scope 'privacy unit' to sufficiently reduce the risk of identifiability. These themes are discussed further in this report.
- Ensuring that the risk of identifiability is not increased by organisations accumulating Stage five output reports over time. These could be combined together, or with other information, to potentially single out people and learn more about their browsing and purchase habits.
- Organisations using PPA will need to carry out an appropriate, continued assessment of identifiability - this includes at different points in time. For example, technological advancements or the presence of additional information can influence the outcome of these assessments.
- Any misuse of the output (eg attempting to identify people, helper parties colluding or manipulation of the histograms) by users of PPA or deviation from its intended purpose may result in the Stage five output not being anonymous.

Privacy and utility

3.22 In Objective four, the ICO and Meta discussed the impacts on privacy and utility when PPA's aggregation methods are applied. For example, differential privacy introduces uncertainty into a dataset by adding 'random noise'. This can help reduce the likelihood that people are identifiable within a dataset. Put simply, more noise makes it harder to ascertain if a person's information is in a dataset. It can also decrease the accuracy of data and the insights that can be derived from it. The epsilon value (sometimes referred to as 'privacy budget') determines how much noise is added. The smaller the value, the higher the level of noise that is added.

3.23 Meta also expressed that it would be ideal for K-anonymity, another aggregation method, to be used in PPA. It aims to ensure that a person's records in a dataset are indistinguishable from at least a number of other records (the value of 'k' minus 1). The higher the value of 'k', the greater the degree of protection. These discussions aimed to provide Meta with feedback to ensure that, when aggregation methods are deployed in PPA, an appropriate balance between people's privacy and utility for advertisers is achieved. The sections below detail some of the feedback provided by the ICO.

3.24 The ICO is not able to provide specific values for key parameters (such as the maximum value of epsilon and the minimum value of 'k' that could be used to provide effective anonymisation). They require a context-specific assessment on a case-by-case basis. This assessment will need to take into account the particular factors including the specificity of the dataset, other available sources of information and the means reasonably likely to be used to identify people. Appropriate values may differ from one context to the next. Appropriate values of epsilon are also currently the subject of ongoing academic research. This point is reiterated in NIST's recent Guidelines for Evaluating Differential Privacy Guarantees.

3.25 The ICO did provide feedback on how these values can be established and the impacts on privacy and utility can be navigated. As a starting point, the ICO recommends that strongly privacy-focussed settings are implemented, supported by empirical testing to demonstrate the effective anonymisation of outputs while still enabling the collection of useful results. This process should iterate through different values of epsilon, converging on the lowest possible

value that still meets these requirements. The ICO also recommended that Meta, and those using PPA, consider publishing an open registry of values organisations have implemented and why they have been chosen. This will help provide accountability and wider scrutiny of the data protection standards organisations have chosen to implement. It will also support consistency in wider attribution modelling.

3.26 The ICO acknowledges that Meta is designing PPA and that it may be deployed by many different organisations. As a result, Meta has indicated that browsers will exercise discretion over various key parameters when those browsers use PPA. The ICO understands there will be no 'one-size fits all' approach. However, the ICO flagged a risk that some browsers could be more committed to data protection than others who could unduly prioritise utility. As such, the ICO suggested Meta explores whether a degree of consensus can be achieved, perhaps via the W3C, to guide key parameters. This could include (but is not limited to):

- acceptable values of epsilon and k that provide sufficient data protection guarantees;
- minimum cohort sizes and whether technical controls can be implemented to protect against attacks on this measure such as a malicious attacker creating fake reports;
- limiting the maximum 'lookback window' to what is necessary, and justifiable from a data protection perspective, to restrict the scope of how much of a person's browsing history is analysed; and
- ensuring that the selected attribution logic (eg last touch or multi-touch attribution) does not result in additional risks to the identifiability of people within the information PPA uses.

3.27 During Objective four, the ICO and Meta discussed the 'privacy unit'. A privacy unit, in this context, means the scope of what is being protected within a dataset. The ICO understands Meta's proposed PPA privacy unit to relate to three dimensions. The first is limiting measurement to a user profile of a single person. The second is restricting measurement to a period of time. The third is applying the privacy budget within the individual website that requests information about impressions (the conversion website). Lastly, aggregation methods within individual browser usage intend to protect insights being drawn in relation to individuals.

3.28 The ICO recommended that Meta ensure the privacy unit is sufficiently wide in scope to protect against certain risks. For example, the time element will need to be sufficiently short to ensure that people with repetitive, continued browsing habits (such as regularly purchasing the same item or providing conversions on the same website) are sufficiently protected from being identified within the Stage five output. The ICO also suggested that applying upper limits to the amount of contributions a person can make to each dataset could help to mitigate this risk in part. Another example is that Meta would ideally have the privacy budget applied across different 'browser instances'. This means that if a person were to use two different browsers or in-app browsers, advertisers would have a separate privacy budget to analyse contributions in each. Meta will need to ensure that any risk of identifiability related to this has been assessed and mitigated. The ICO also queried whether this risk may be relevant to social media use, such as whether impressions and conversions might be measured both in the browser and within a dedicated app, and whether they would have separate privacy budgets.

3.29 A further risk exists, which will need to be mitigated, in relation to groups of websites or those with agreements or relationships such as shared ownership. For example, they may be able to correlate their activity to understand the browsing behaviour of a single person across multiple websites. Safety limits which operate as additional privacy budgets, and are not applied at an individual site level, could help to mitigate this risk.

3.30 The ICO is encouraged that Meta's designs included a commitment to include additional security measures. One approach Meta is considering is using rate limits. These would aim to restrict the possibility of misuse of PPA by limiting the speed at which websites can consume the privacy budget. The ICO views this as a good inclusion as part of a wider set of measures. The rates will need to be tested to ensure that they are set to provide appropriate security. Any safety limit budgets (as described above) would need to be set appropriately to ensure rate limits are effective. These measures will also need to be kept under review over time.

3.31 Similarly, Meta has identified a risk that individual sites or groups of sites might be able to split themselves up into smaller sites with different domains. This means they could use those additional entities to misuse the privacy budget if each sub-site is assigned its own. Meta believes that this type of behaviour would be detectable and mitigated by the various protections that are built into PPA. Meta also says that internet browsers deploying PPA will need to

analyse the use of PPA to identify unusual or changing patterns to identify risks such as this. This type of vulnerability should also be assessed in relation to how organisations are already set up and established (eg across different sites and domains), and not just from the perspective of potential malicious attacks. The ICO has encouraged Meta to consider how it will communicate about these types of risks with browsers. This includes considering how it might make recommendations to browsers to detect and mitigate these types of risks. As an additional deterrent, Meta has suggested that browsers could block sites that are detected using such malicious attacks from using PPA.

Governance framework

3.32 The previous section of this report primarily focusses on some of the technical measures Meta intends to implement to help protect people's information that PPA uses. To supplement PPA's technical measures, Meta intends to develop and implement a governance framework to help provide further protection. This framework will include contractual measures and terms and conditions of service. The ICO's guidance on effective anonymisation techniques makes it clear that contractual, technical and organisational controls all play a part within a wider assessment of effectiveness.

3.33 Objective five of the Sandbox plan was originally intended to focus on the helper parties providing the MPC function. In addition, the ICO and Meta also considered the potential governance framework more widely across the potential use of PPA. Meta's plans in relation to this governance framework were at an early stage during Sandbox participation. As such, this objective intended only to discuss possibilities and to flag potential risks. Discussions took place during a workshop at Meta's London office on 29 April 2025. The sections below outline some of the themes that were discussed.

3.34 The ICO takes a positive view of Meta's intention to implement contractual stipulations that are designed to prevent behaviours that negatively impact the risk of identifying people. For example, Meta has suggested that measures to prevent collusion between the MPC helper parties to reidentify people could be implemented. Meta has also suggested that the helper parties could be restricted from combining information from PPA with information they hold themselves for their own purposes. Both of these ideas could provide additional levels of protection.

3.35 However, the ICO recommended to Meta that it will need to assess whether contractual stipulations are sufficiently wide in scope to capture the broad range of behaviours that could result in the misuse of PPA. This could include detailing specific misuses but also ensuring that all potential misuses are appropriately deterred. The ICO also suggested, at various points during Sandbox participation, that contractual stipulations could be used to add protection more widely. They could be implemented into terms and conditions of service related to other parties using the service. For example, terms and conditions could be used to ensure that browsers deploying PPA implement appropriate levels of differential privacy parameters, aggregation and additional safety limits. Maximum lookback windows could be established. Organisations could be required to ensure that their use of PPA is restricted to its specific stated purpose. Advertisers could be prohibited from accumulating Stage five outputs over time with the intention of combining them to identify people.

3.36 Meta stated that it is considering a range of penalties for breaches of contractual stipulations. This could include audits and reassessment of the relevant organisation's suitability to use PPA. They also could include temporary and permanent disqualifications from using PPA and financial penalties. Meta intends for these to be used proportionately in relation to the severity of the offence. The ICO suggested that Meta will need to consider how misuse will be monitored, and who will be responsible for detecting it and enforcing any penalties. There should also be clear criteria related to how the severity of misuse will be judged.

3.37 The ICO considers that the continued critique and scrutiny of the governance framework is important. It may help to ensure that the governance framework continues to evolve appropriately and produce recommendations for further development from a range of stakeholders. Publishing the governance framework, perhaps via a vehicle such as the W3C, and inviting consultations may help to obtain that scrutiny. The ICO also acknowledges that, given Meta's position in the AdTech sector, its governance measures could involve it affecting commercial freedom and wider outcomes for firms, including competitors. It will therefore be necessary for the design and operation of governance measures to take into account the need to comply with competition law.

3.38 Meta has indicated that it could implement an accreditation process. This would mean that organisations wishing to participate in the use of PPA with Meta would need to meet pre-determined standards, for example set by an

independent standards group or body. The ICO has not seen any documentation relating to this proposed process, given the early stage of development of the governance framework, during Sandbox participation. However, assuming it works appropriately and is effective in helping ensure data protection standards, this approach may help support the wider governance framework. Considerations, such as ensuring the process is sufficiently robust, how it will be resourced and enforced, and the regularity of renewing accreditations appropriately will need to be assessed.

3.39 Related to this process, Meta proposed that a list of approved helper parties could be created. Organisations deploying PPA would then be able to select a combination of two helper parties to perform the MPC function. The ICO recommended that Meta consider whether it can add any further protections in relation to this selection of helper parties. For example, it could consider introducing requirements that there are no conflicts of interest with the helper party pairings. If Meta assesses that this will reduce the risk of collusion and combining information between helper parties it may help add additional protection. The ICO also flagged a risk that MPC parties could merge. As it designs PPA's governance framework, Meta will need to assess how organisations would respond if two helper parties merged, both pre and during PPA's use.

3.40 During this objective, the ICO reiterated that it is important to ensure that PPA is used transparently. As a developer of PPA, Meta can assist with the transparency efforts of those that deploy PPA. Meta has stated that it is committed to transparency efforts. Providing appropriate levels of transparency could be included within aspects of the governance framework such as terms and conditions of service. The ICO and Meta also discussed how PPA involves very complex processing operations which may not be immediately understandable. The ICO recommended that Meta could consider providing explainable videos or visuals that help supplement wider transparency methods. The benefits of ensuring good data protection standards should also be explained. For example, aggregation methods with appropriate levels of privacy protection could also benefit utility for advertisers.

3.41 The ICO also views that Meta, as PPA continues to evolve in the future, should continue to keep its designs publicly available. This could help to contribute to efforts to comply with data protection law's requirements on transparency, accountability and data protection by design and default. Relevant bodies, such as the W3C and perhaps any appropriate standards bodies that do not have a direct interest in PPA's development, should be engaged with to

provide additional oversight and scrutiny. These could include bodies such as IAB, IETF, NIST or ISO where appropriate. Meta could also make it clear where changes are made and what their impact on data protection would be. Meta could use consultations to provide structured feedback processes, including where any changes impact data protection standards or privacy.

4. Ending statement

4.1 By engaging with the Sandbox, Meta has had the opportunity to engage with wider ICO expertise to help understand where UK data protection laws will apply to the use of PPA at a granular level before it is deployed. The ICO has helped Meta consider how it will achieve an appropriate balance between privacy and utility in relation to how it will implement its aggregation methods. The ICO has supported Meta in thinking about how its proposed governance model can add additional protections for people and also identified some risks which will need to be mitigated. This has helped to provide regulatory certainty to Meta as it researches a system that it intends will both ensure user privacy and enable effective online advertising measurement.

4.2 The ICO's report on tackling barriers to PET's adoption indicates that the uptake of PETs across many sectors is low. The ICO is encouraged that Meta, a global organisation, is researching how PETs could be implemented more widely across the online advertising industry. This Sandbox project provides a use case as an example of how some of the barriers to responsible PETs adoption may be overcome. For example, it demonstrates how PETs could be integrated into complex systems. It also demonstrates how PETs can form part of a wider data governance framework instead of being an isolated technological intervention. The ICO's PETs guidance, finalised anonymisation guidance and encryption guidance also provide further legal clarity in this area.

4.3 This Sandbox project has helped the ICO to further develop its knowledge and demonstrate a practical application of certain themes related to its anonymisation, PETs, differential privacy and MPC guidance. For example, it has provided an opportunity to consider the risk of identifiability of data processed within MPC systems. It has also helped the ICO

to assess and document some of the technical and organisational measures that could help to mitigate the risks associated with systems such as those using differential privacy and MPC.

4.4 Online tracking is a strategic priority area for the ICO. The ICO has recently called for views on how it regulates online advertising. This includes reviewing its approach to enforcement of the PECR regulation 6 requirements. This is to enable new commercially viable ways to deliver online advertising. The ICO has not yet formed a position on what will be included in any proposed enforcement approach. However, this work has contributed to the ICO's understanding of potential emerging new solutions.

4.5 Engaging with projects such as this which intend to implement PETs into their designs demonstrates the ICO's commitment to exploring how PETs could be used in industry. It underlines the ICO's status as a trusted information rights regulator. Exploring challenging Sandbox projects further highlights the ICO's commitment to its objective to empower responsible innovation and sustainable economic growth within its ICO25 strategic plan.

4.6 Following the completion of its Sandbox participation, Meta stated that "The publication of this report is the result of over a year of information-sharing with the ICO. The final report highlights the regulatory considerations that need further focus. We will continue to work on the PPA proposal via the W3C with the ICO guidance in mind."