PERSONAL DATA PROTECTION COMMISSION SINGAPORE

PRACTICAL GUIDANCE TO META

Background

1. Meta is implementing a Proof of Concept (POC) on Interoperable Private Attribution (IPA) to measure the effect of advertising impressions on conversions without the use of 3rd party cookies or mobile device identifiers[1].

2. The IPA solution architecture [2] in Meta's POC uses Privacy Enhancing Technologies like multiparty computing (MPC) and differential privacy (DP) to generate an attribution report for measuring advertising impressions and conversions.

3. The key stakeholders in Meta's IPA solution architecture are:

a) **Publisher** – an organisation that owns or supplies digital advertising space (e.g., social media website, news publishing sites, software platforms)
b) **Advertiser** – an organisation that buys digital advertising space for their marketing campaigns (e.g., brand owners)
c) **Adtech Entity** – an organisation that provides services to brands associated with creating, planning and managing advertising campaigns
d) **Platform Provider** - which may be one of:
    a. **Browser Vendor** – an organisation that develops or provides internet browsing services
    b. **Mobile OS vendor -** an organisation that develops or provides a mobile operating system for which developers create internet-connected applications.
e) **Helper Party** – an organisation that performs the MPC. The IPA architecture uses three Helper Parties for the MPC.

4. A brief description of the use case and attribution report generation process in the POC is as follows:

a. **Determining activity data fields for attribution measurement.** Advertiser runs an advertising campaign for its advertisements on Publisher's website/app. Publisher displays the advertisements to its users, a proportion of which would proceed to the Advertiser's website/app either to browse, and/or to make a purchase. Advertiser engages the Adtech Entity to

[1] While the POC that was tested did not involve modifying browsers or mobile operating systems, the simulated data had the same format as per the specifications for key generation for a browser or mobile operating system in the IPA proposal.
[2] Details on Meta's IPA solution is explained through https://github.com/patcg-individual-drafts/ipa/blob/main/IPA-End-to-End.md

measure the conversion value attributed to the Publisher for the advertising campaign. Advertiser and Publisher agree on the relevant activity data fields needed for attribution measurement specific to this advertising campaign. For the POC, the agreed activity data fields for attribution measurement do not include any information that can directly identify an individual (e.g., name, mobile number, email address).

b. **Generation, shredding and encryption of browser/device[3] key.** A unique browser/device key will be generated for each user upon installation of the browser or mobile operating system. This browser/device key permanently resides with the user (i.e., generated and stored in the user's device), and will not be accessible by the Platform Provider or any party. The browser/device key will be "shredded" into three random[4] secret shares, and encrypted to generate a set of three encrypted secret share pairs (**ESSPs**[5]) for each browser/device session. Each ESSP is encrypted with the public key of one of the Helper Parties according to the IPA protocol such that each Helper Party can only decrypt its assigned ESSP.

c. **Generation of activity data alongside ESSP to be shared with Adtech Entity.** The Publisher and Advertiser will each extract the relevant/agreed activity data fields for attribution measurement and append the ESSPs before sharing with the Adtech Entity for sorting and filtering purposes.

d. **Shredding of activity data into activity data secret share pairs for MPC.** The Adtech Entity will sort and filter the necessary activity data before "shredding" them into three random secret shares. Each pair of activity data secret shares (similar to the implementation of the ESSPs) will be shared with the corresponding ESSP to the respective Helper Party.

e. **Generation and sharing of desired attribution report.** Each Helper Party processes the activity data secret share (i.e., using MPC and DP noise) to generate two "shreds" of the attribution report which is then shared with the Adtech Entity. The Adtech Entity merges the three unique "shreds" of the report to generate the desired attribution report. The attribution report is shared only with the Advertiser and Publisher.

5. Meta sought Practical Guidance (Guidance) from the Personal Data Protection Commission (PDPC) on the following:

a. Whether the data involved in the POC constitutes anonymised data[6], for which the Data Protection Provisions under the PDPA do not apply.

b. Roles and responsibilities of key stakeholders (see **paragraph 3** above) under the PDPA.

---

[3] Browser key would be used by website while device key would be used by mobile application.

[4] Randomness is based on the Cryptographically Secure Pseudo-Random Number Generator (CSPRNG) function of the operating system

[5] Based on Hybrid Public Key Encryption (RFC 9180)

[6] Anonymisation refers to the process of converting personal data into data that cannot identify any particular individual and, depending on the specific process used, can be reversible or irreversible.

c. Additional safeguards and considerations to lower the risk of identification and re-identification.

PDPC's assessment

6. PDPC's Guidance set out below will be based on the assumption that the activity data fields shared by the Publisher and Advertiser with the Adtech Entity for attribution measurement will involve personal data.

7. PDPC considers the key Privacy Enhancing Technologies (PET) involved in the IPA architecture detailed in paragraph 4 to include:

a. Paragraph 4b: Anonymising the generated browser/device key by "shredding" and encrypting the browser/device key into 3 secret share pairs (ESSPs) accessible only by respective Helper Parties based on the IPA's protocol.
b. Paragraph 4d: Anonymising activity data by shredding of activity data into pairs of secret shares accessible only by respective Helper Parties based on the IPA's protocol.

8. In general, PDPC uses a risk-based approach in determining whether data is anonymised, and it will depend on the circumstances in which the data is being collected, used and shared. Data that has sufficiently low risk of re-identifying any individual will be considered anonymised data under the PDPA[7]. Based on the design of the IPA POC, no Helper Party will be able to know the browser/device key or activity data in its entirety, unless any Helper Party is able to access and combine any two of the three secret share pairs. The guidance below provides PDPC's recommendations on some of the technical, governance and process safeguards that can be put in place by each stakeholder to lower the risk of re-identification.

Roles and Responsibilities of each stakeholder in the POC

Publisher and Advertiser

9. Based on the information detailed in **paragraphs 3 and 4, and the considerations in paragraphs 6 to 8**, PDPC is of the view that the Publisher and Advertiser are data controllers (DCs), which are in possession of activity data they each collect from individuals, a subset of which they would share with the Adtech Entity for the generation of the desired attribution report. The generation of attribution report is for both the Publisher's and Advertiser's purposes (i.e., to measure effectiveness of advertising campaigns).

10. As DCs, both Publisher and Advertiser should assess and minimise any downstream risks of re-identifying any individual by other stakeholders or unauthorised parties from the activity data shared and the generated attribution report.

[7] Refer to Section on Anonymisation in **Advisory Guidelines on the Personal Data Protection Act for Selected Topics** and PDPC's **Guide to Basic Anonymisation.**

a. In determining the activity data fields to be used in generating the attribution report, both the Publisher and Advertiser should apply the principle of data minimisation based on the intended structure of the agreed attribution reports to select only data fields that are relevant to the reports. Where possible, they should remove any direct or common identifiers that are tagged to any individual (e.g., campaign IDs specific to individuals or customer IDs) and consider using activity data fields that are less likely to identify any individual.

b. In determining the structure and quantity of the attribution reports to be generated by the Adtech Entity, the Publisher and Advertiser should consider whether the generated reports (individually or in aggregation) may result in disclosure of any of their customers' personal data and take reasonable measures to reduce the risk of such individual linkage (e.g. transaction value made at Advertiser's website/app by a specific individual which is tagged with a specific campaign ID is disclosed to Publisher via the generated report(s)). In cases where the generated attribution report(s) can be used to reveal personal data about an individual to the other stakeholder (i.e., Advertiser or Publisher), it will be considered disclosure of personal data for which consent is required, unless any of the exceptions provided in the PDPA apply.

Adtech Entity

11. PDPC views the Adtech Entity as a data intermediary (DI) that processes personal data (i.e., sorting, filtering and "shredding" the activity data) on behalf of and for the purposes of both the Publisher and Advertiser. PDPC has given guidance that express consent is not necessary for an organisation to share personal data with its DI to process personal data on its behalf, provided that the personal data is not used by the DI for other purposes without the consent of the individual[8]. As such, **consent is not required for the Adtech Entity to collect (from the Publisher and Advertiser), sort, filter and "shred" the activity data for the purposes of generating the attribution report for the Publisher and Advertiser.**

12. Nevertheless, as a DI, the Adtech Entity will be subject to the Protection, Retention Limitation and Data Breach Notification Obligations under the PDPA[9]. For avoidance of doubt, where the Adtech Entity uses the activity data beyond what is required and agreed with the Publisher and Advertiser, the Adtech Entity will be considered a DC in relation to the activity data, and all PDPA Obligations will apply (including the need to obtain consent from the individual to collect the activity data from the Publisher and Advertiser).

[8] See PDPC's **Guide to Data Sharing**, at para 1.8.

[9] For instance, the DI will need to ensure that the personal data it collects and anonymises on behalf of the Publisher and Advertiser is adequately protected, and not retain the personal data for periods longer than necessary. The DI is also required to notify DCs without undue delay from the time it has credible grounds to believe that the data breach has occurred.

Platform Provider

13. In the IPA implementation, the browser/device key is intended to be kept hidden from any parties and will not be combined with any data that the Platform Provider or any other third parties may have, to identify the user. As such, the **Platform Provider's generation of the browser/device key will not constitute collection of personal data.** The "shredding" and encryption of the unique browser/device key will also not constitute use of personal data, and the Data Protection Provisions under the PDPA will not apply.

Helper Parties

14. **PDPC considers the output from PET implementation (detailed in paragraph 7 and 8) to be anonymised data,** so long as the risk of re-constructing the browser/device key and activity data from the data remains reasonably low. This risk should be assessed in conjunction with any technical, governance and contractual safeguards implemented system-wide in the IPA implementation.

15. Based on the activities undertaken by the Helper Parties in the POC (i.e., collecting activity data secret shares and corresponding ESSP from the Adtech Entity, and processing the data as described at **paragraph 4d**), the Helper Parties will be considered to be processing anonymised data and thus not be subject to the PDPA.

Safeguards and Considerations to lower risk of identification and re-identification

16. Given that the browser/device key is designed to be permanent and unique, it has the characteristics of an identifier which could be used by various websites/apps to combine other information about the user. This increases the likelihood of the browser/device key being personal data. Additional safeguards that lower the risk of identification may include, for instance:

a) Ensuring that the browser/device key is generated and used only for the attribution report. It may also be worthwhile considering whether a temporary browser/device key can be deployed instead (e.g., imposing a validity period and re-generation cycle for each browser/device key).

b) Ensuring that the techniques used in the "shredding" of browser/device key and activity data are sufficiently robust to prevent the same key "shreds" from being generated at both Publisher and Advertiser's end, as well as threat actors from being able to execute an attack (e.g., rainbow table attack) to precompute possible key "shreds" and combinations. Where possible, these techniques (including encryption) should be aligned with industry standards (e.g., using encryption protocols widely accepted by industry to be secure).

17. Apart from the risks of identification arising from the use of browser/device key as an identifier, there are also risks of re-identification of individuals due to the critical role the Helper Parties play in the IPA solution architecture. Additional safeguards that may be put in place to lower the risk of re-identification may include, for instance:

a) Ensuring that Helper Parties do not attempt to collude or re-identify any individual from the anonymised data through contractual means and other governance obligations (e.g., audits). Technical safeguards (e.g., programmatic guardrails) can also be explored to prevent or red-flag possible collusion between Helper Parties.

b) Ensuring that Helper Parties put in place baseline governance and technical implementation measures to protect and secure their secret keys from unauthorised access/compromise (e.g., industry-recognised processes and standards such as ISO and NIST).

END OF DOCUMENT