



List of questions – TrusPID Meeting 03/03/23

Global perspective

- Can you send us a complete list of all partners, publishers, etc., and a complete list of all websites taking part in TrustPID?
- Is there any connection between TrustPID and Open Gateway?

Technical details

- Can you explain in detail how each ID is generated? What data is included, e.g. hashes of what data?
- 
- 
- Do web pages contain code or images or similar from a TrustPID host when using TrustPID? If so: which host?
- Will usage data of several users be mixed when using a connection together, e.g. in a mobile tethering situation?
- What measures are taken against the request of IDs from an unauthorised app, unauthorised website or malware without asking for consent?
- Is there also the possibility that these third parties can then view and modify information in TrustPIDs privacy portal?

Consent collection and legal basis

- When visiting a website, is the user redirected to TrusPID or other intermediary (specify) in order to give consent or is this consent being relied upon from the initial publisher site?
- For what do you collect users consent? Can you share the consent text currently being used?
- When you gather user consent, how can you inform the user of the identity of the joint controllers (brands and media) that will change over time?
- How does the consent collection work in the context of a user using different browsers on a single device? Will he get the same identifier on both?
- From your document: "when a Movistar customer for example visits Zara via two browsers, Zara regards him/her as two different people, which may be detrimental, as the customer in question is individualised incorrectly. In these cases, the customer can't benefit from a more personalised Zara advertising campaign, as the campaign is limited by the above factor. However, TrustPid provides Zara with a pseudonymous identifier so that, even though the user gains access via two devices, it knows that he/she is, in fact, a single person."
Could you explain the last sentence which seems to contradict what is said above? Do you consider two browsers on a single device or two devices on a single connexion?
- How do you plan to check that the contractual obligations for obtaining consent are being followed by the websites? How do you ensure that valid consent is obtained and typical mistakes often seen in consent banners are not made by your partners?

- More generally, you are relying a lot on the contracts with all processing parties to have the TrustPID-processing taken place. Which specific safeguards have been put in place within these contracts, what are the consequences of not following the binding contracts?
- You mention that there would be as contractual safeguard not to process any special category of data. Does that mean that none of the websites using TrustPid could offer services linked to health, sexual life, etc.?
- Does the user still have full access to the site content if he rejects consent?
- Do you think that there is a risk for the unambiguous and informed nature of the consent when the user, even if he opted out, is presented with a consent screen on each page implementing TrustPID?
- The IP-Address is transmitted to TrustPID / VSSL to check whether TrustPid can be used with the internet access. What is the legal basis?
- Could an anonymised IP address also be used, e.g. 47.11.12.xx or 4711:abcd:1234:xxxx.. ? This should also clearly identify a network operator, but not a user.

Data collection and identifiers lifecycle

- Is it possible for users to trigger a new generation of IDs at any time? If so, how? Is it possible for users to access their identifiers?
- What types/categories of data are associated with the ID relating to a user? Is a profile of interests built up over time?
- A user visits two sites: first site A and then site B. How do you know that he has visited both sites? What kind of information you deliver to site B (concerning prior visit to site A)?
- The MarTech identifier changes every 90 days, is that correct? How are third parties prevented from using other identifiers (login data, cookies, etc.) to connect two subsequent ID to the same user?
- Will the period for changing [REDACTED] remain permanently at 90 days or is there a risk of significantly extending this period?
- How do you manage the risk of excessive collection of [REDACTED] by the DSP?
- Is there a minimum size for a segment to be valid (for example more than 5000 person)?

About the DPIA

- Is the legal basis in the DPIA on page 9 point 1 in the graph correct?
- On page 15 there seems to be a contradiction. Above, under 1. it is stated that consent is given first. In the table under 2.9 it says "before consent". Could you clarify this point?