TrustPid

Main privacy and personal data protection aspects

February 2023

Contents

1. Introduction and goals

The TrustPid project is seriously committed to the strictest compliance with data protection laws in all countries, and in particular taking into account Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter, "GDPR") and the Privacy and Electronic Communications Directive 2002/58/EC on Privacy and Electronic Communications ("ePrivacy Directive").

The requirements and obligations for the data controller laid down in the GDPR include the principle of proactive accountability, which entails the need for the data controller to implement the appropriate technical and organisational measures to guarantee and demonstrate to the data subjects and the supervisory authorities that the processing is compliant with the GDPR.

This document, together with the proactive engagements held with relevant regulatory data protection authorities prior to any processing being undertaken in specific markets, offers proof of the TrustPid project's diligent compliance and respect for the principles of privacy by design and privacy by default, as set out in the applicable legislation.

What follows is an executive overview of the main privacy and personal data protection issues raised in TrustPid's pilot phase (as defined below), listing all the stakeholders involved, the purposes pursued and the kinds of processing operations carried out, as well as the key measures taken to ensure compliance with the GDPR and ePrivacy Directive and respect for the data subjects' right to privacy and data protection. Once the pilot phase of TrustPid is completed, the commercial phase will begin, which will involve certain changes, such as the role of VSSL being taken over by a Joint Venture made up of the four main European carriers (Deutsche Telekom, Vodafone, Orange and Telefónica).

Therefore, this document serves as a further resource to demonstrate the due diligence in compliance with the GDPR, a resource that will make it easier for the reader to learn more about and understand the most significant aspects of TrustPid and the roles of the different stakeholders (as listed below). This is in addition to the other resources that are available and/or required by the GDPR, such as the Data Protection Impact Assessment carried out by VSSL (as defined below) and reviewed by the other parties, which is also made available to the relevant data protection authorities together with any other documentation that may be requested.

2. Definition of TrustPid

"TrustPid", also known as "Telco ID" and "Argus Project", is the name of a **network-based online identification service** which has been developed with the intention of addressing the multiple privacy issues currently affecting the digital advertising industry in Europe. Specifically, TrustPid seeks to provide greater security, user control and transparency for digital advertising activities by operating solely upon the basis of prior user consent, direct contractual relationships with each entity involved in the service provision, centralised privacy preference management and data minimisation.

TrustPid, led by the main European telecommunications carriers or "Telcos" (Vodafone, Deutsche Telekom, Orange and Telefónica), uses a technology **based on the Telcos' ability to create a unique identifier associated with the different public IP addresses** used by a single internet access point (mobile only during the pilot phase), with the potential to **enable use cases with commercial and business value for third-party companies** (e.g., advertisers and online media).

[redacted] This linking activity is already performed by Telcos for the purpose of undertaking different specific processing operations that the carriers are required to perform under the telecommunications service contract with their customers (e.g., service provision, billing, etc.). In this regard, TrustPid is a value-added service whereby the additional benefit provided to the users is empowerment or greater control and transparency in relation to the processing of their data within the context of online advertising.

TrustPid is currently undergoing its pilot phase in Germany for a "re-targeting[1]" advertising use case. This pilot will soon be extended to Spain and France, The service will then be put into final production and marketed through the above Joint Venture which is currently being created.

During the pilot phase, the solution is **designed to allow the personalised advertising activities for re-targeting to be conducted in a more secure and transparent manner whilst enhancing individuals' choice and control** over the required personal data processing. In this respect, as will be outlined below, the users will obtain clearer information as to what personal data processing is necessary to receive personalised advertising as part of the consent collection and, furthermore, they will be able to determine which third parties can provide them with personalised online experiences and when they want the processing to cease in each particular case.

3. The main TrustPid stakeholders and their role from a standpoint of data protection

- The **Telecommunications Carriers** (also known as "Telcos") participating in TrustPid (currently Vodafone, Deutsche Telekom, Orange and Telefónica), the data controllers, the receivers of the public IP of the user to be identified, together

[1] "Re-targeting" can be defined as a digital marketing or advertising initiative that consists of sending messages and adverts to users who have visited or interacted with a specific website on other web pages.

with certain data associated with his/her browsing (to be subsequently specified), and the providers of the pseudonymous identifier generated by the Telco [redacted] of the user who consents to the use of TrustPid and, in turn, is a customer of a participating Telco, in order to allow VSSL to provide the online identification service to Media and Brands.

- **Vodafone Sales & Services Limited ("VSSL")**, a UK company in the Vodafone Group under identification number 06844137, with its registered office at Vodafone House, The Connection, Newbury, Berkshire, RG14 2FN, England.

  VSSL is the data controller, [redacted], and its role is to provide the TrustPid online identification service to Media and Brands and the centralised permissions management service to the users.

  In the future, VSSL will be replaced in full in its functions by the Joint Venture ("JV") which is currently being jointly incorporated by the Telcos (Vodafone, Deutsche Telekom, Orange and Telefónica), following the antitrust approval from the European Commission.

- † [redacted]

- [redacted]

- [redacted]

- "**Media"** (also referred to as "publishers") attached to TrustPid, as joint controllers with VSSL. They are the owners of the websites on which the users browse and interact and on which the consent of the latter is gathered for the personal data processing operations required for the functioning of TrustPid.

[2] MSISDN stands for Mobile Station Integrated Services Digital Network and refers, in practice, to a user's telephone number.

- **“Brands”** (also referred to as “advertisers”) attached to TrustPid, as joint controllers with VSSL. They are the owners of the websites on which the users browse and interact and on which the consent of the latter is gathered for the personal data processing operations required for the functioning of TrustPid.
- **“Users”** who browse the websites of the Media and Brands attached to TrustPid as data subjects whose data are processed and who, from the standpoint of the Telcos’ involvement in TrustPid, will be customers of the mobile internet service of the participating Telcos.
- **“AdTech Vendors”**, stakeholders who are usually involved in the online advertising industry processes and used and hired by the Brands, the Media and VSSL for such a purpose as Demand-side Platforms (DSPs), Supply-side Platforms (SSPs) and Data Management Platforms (DMPs). Specifically: (1) the SSPs allow the Media to offer and market their advertising spaces, (2) the DMPs allow the Brands to profile the users who access their websites and (3) the DSPs allow purchases of the advertising spaces offered by the Media via their SSPs.

4. Value proposition

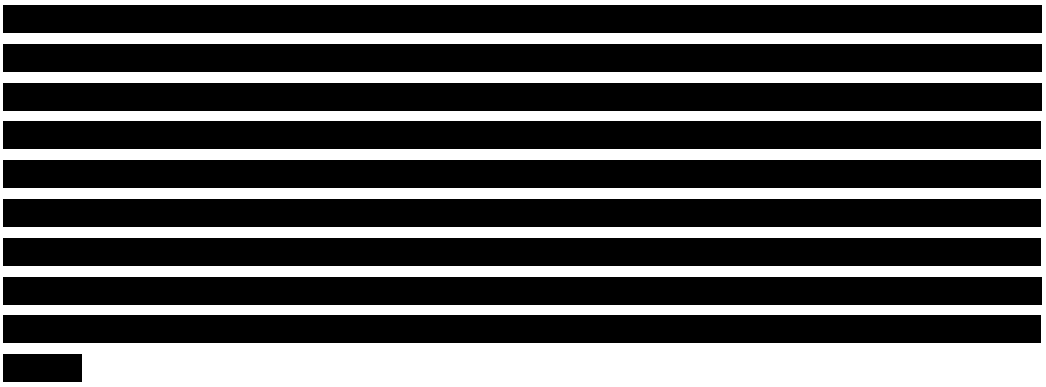
TrustPid is a project designed to provide an online identification service for users of Brands and advertisers [redacted] and the Media and publishers [redacted] advertising purposes.

The online advertising sector needs a new way of identifying users in a manner which is more respectful of their privacy while overcoming all the drawbacks stemming from the disappearance of third-party cookies. We can summarise them as follows:

- **Advertisers** are looking for an online identity product that enables them to:
  - **Show adverts to users who have a real interest in their brand** (they’ve visited the advertiser’s website);
  - **Limit the number of adverts** shown to each user;
  - **Personalise the experience** on their website.
- **Publishers** also need an online identity product that:
  - Helps them to improve their website so as to **personalise the content for each user and make their advertising space more attractive to advertisers**;
  - **Allows independent AdTech providers to compete with Google** and thus reduce the latter’s power in the market.
- **Users** are confused about when and how their personal data are used. They understand that a large part of the Internet is free of charge due to advertising, but they need more:
  - **Control over who has permission to process their personal data and show them** personalised **adverts and contents**;
  - **Transparency about how the above is done**.

- **Telcos** can use the users' IP addresses to help to create a solution that benefits users, advertisers and publishers. The main **differences between them and** cookies are that:
    - Users can revoke **the consent given to each brand and publisher via a centralised Privacy Portal**;
    - The consent must be given vis-à-vis each website (Brand and Media) in order to enable the service, and therefore it doesn't **extend to other websites and can't be shared by Brands and Media**;
    - Everyone benefits from the **improved data quality**;
    - It's a **more transparent system for the user,** who is provided with detailed information on the data processing involved via different means, such as the centralised Privacy Portal and the privacy policies of the stakeholders.

TrustPid therefore enables the Brands that use it to resolve the problems and limitations of the current cookie-based identification solutions available to advertisers and publishers.



This technology also promotes **digital sovereignty** for the user by enabling users to have greater control over their privacy preferences by virtue of having access to a **centralised privacy portal** via which they can view and manage the above preferences in one place without having to remember or re-visit the websites to which they previously gave their consent. Currently, if a user gives their consent to cookies on random websites and then closes them, after a while they would not be able to remember all the websites to which they have consented. Meaning, although they have the right to revoke their consents, they are unable to do so unless they remember each website visited and consented to. This leads to a situation where the user has various consents still active in the internet. In the case of TrustPid, the privacy portal gives the user the ability to see and control their consents given under TrustPid for each website they have ever visited, whenever he likes. The Privacy Portal enables users to revoke all the consents given in one place and with one click, as well as individually per website, thus bringing a greater level of control back to the user.

TrustPid is configured as a **project with a significant capacity to shape the European Telcos as relevant actors in the online advertising market, characterised by its importance in terms of income, in which the Telcos have traditionally played a secondary role**, mainly as advertisers and publishers.

5. Categories of personal data

TrustPid **will not process any personal data that can directly identify users**. **Only pseudonymised personal data relating to users' online identifiers and certain data associated** with their browsing **will be processed**. Specifically, if they are categorised in accordance with their origin or provenance, the following categories can be distinguished:

- Data from assignments made by other data controllers/data captured without the user's involvement:
  - **Public IP of the user browsing the publisher's or advertiser's website**. [redacted]
  - **Contextual browsing data associated with the public IP**, [redacted]
- Data assigned to and/or generated by the user:
  - [redacted] **the generated pseudonymous identifier of each customer of the carrier**, [redacted]. During the pilot phase, [redacted]
  - **Unique online identifiers of the user of the online advertising environment**. These identifiers are digital tokens randomly assigned to each user for the purpose of deploying the use cases. They are mainly the [redacted] MarTech ID and AdTech ID. [redacted] of the identifiers are persistent and, in any event, those accessible to brands and publishers, do not provide a complete picture of the data subjects' browsing or interests.

The Brands and Advertisers may, under their sole liability and in compliance with the obligations laid down in the data protection legislation, carry out additional personal data processing consisting of the profiling of the identifiers received in order to run personalised advertising campaigns.

The relationship with the Brands, Advertisers and Media is maintained by VSSL and the corresponding contracts are entered into for it, establishing all the necessary guarantees in terms of regulatory compliance with regard to the use of the digital tokens.

6. Purpose and processing operations performed

The purpose of TrustPid's processing is to **identify the customers of each Telco on the websites of the brands or media that subscribe to the solution** by using encrypted or pseudonymised data in order to enable use cases with commercial and business value for said brands or media, enabling them to **(i) perform commercial profiling and (ii) display advertising, products and personalised contents**.

With respect to the different processing operations, TrustPid proposes the following chain of actions:

- Through VSSL, [redacted] (when they access their services and after they give their prior consent). [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

TrustPid therefore entails a series of processing operations with the aim of providing an online identification service to advertisers and publishers, whilst providing users with greater control and transparency with regard to the processing of their personal data and, at the same time, make their targeted online advertising more effective. The Telcos, for their part, are involved in some of these processing operations, as indicated above.

7. Lawful basis

The lawful basis for the processing and assignment of data in TrustPid is the **user's free, informed and specific consent**, the collection of which is separately delegated to the advertisers and publishers on and for each website of said advertisers and publishers attached to TrustPid just before the processing begins, [redacted]

This consent is given for all the data processing operations which are indicated, including the processing of traffic data for the provision of a value-added service to the Telcos' customers within the meaning of the provisions of the ePrivacy directive currently, data sharing between the stakeholders involved in the project and the use of first-party cookies and the profiling carried out by the Brands, as outlined above.

In TrustPid it's **just as easy to give the consent as it is to deny it via the dedicated TrustPid consent pop-up in participating brand or media sites, on which the user can deny the consent with respect to the specific Brand or Media with a single click. The user can also easily withdraw any consents given in relation to TrustPid either directly on the relevant brand or media site, or centrally via a privacy portal (www.trustpid.com) on which the users can manage all the consents they have given in one place**. This portal will be accessible: (i) directly via the browser, browsing in said website domain, (ii) on the brand or media banner on which the consent is received, (iii) in the information sections that the Telcos and Brands and Media have enabled for the purpose. In addition, in the footers of the brand and media websites, the users will have the option of revoking their consent without having to go to the privacy portal.

In addition, some Telcos, on an individual basis, may establish an additional transparency measure whereby, [redacted]

[redacted]

In order to manage their consents on the TrustPid Privacy Portal, [redacted]

VSSL has contractually established obligations for the Brands and Media in relation to obtaining consent to ensure that the consents are properly gathered. Similarly, VSSL conducts weekly inspections of the implementation of the TrustPid consent pop-up on the websites of the Brands and Media to verify the validity of the consents.

8. Transparency

As shown in Annex I, TrustPid incorporates a layered information system for the purposes of complying with the transparency obligations laid down in articles 13 and 14 of the GDPR and following the guidelines and recommendations of the EDPB and the data protection authorities. It should be borne in mind that special emphasis has been placed on ensuring that the users are provided with various channels via which they are given clear information with respect to how TrustPid works, what personal data processing the system entails and how they can manage the consents they give:

- [redacted] included on the websites of the Brands and Advertisers, as well as referenced on their privacy statements.
- On the TrustPid Privacy Portal.
- By means of mentions provided by the Telcos in their privacy policies and transparency centres,

Particular emphasis has also been placed on using clear and simple language to enable the data subjects to fully understand the processing operations to which they give their informed consent.

9. Risk analysis

Given the convergence of the personal data processing operations required of the different stakeholders for the operation of TrustPid, said stakeholders have decided to conduct a joint risk analysis in the field of data protection in order to assess the potential risks of such processing in a comprehensive manner, without detriment to the fact that, at the same time, each of these stakeholders may decide to carry out specific risk analyses for their areas of responsibility. Given that this is an international project involving different jurisdictions and supervisory authorities, the joint risk analysis has been worded in English.

As a result of the joint risk analysis conducted in TrustPid's impact assessment, the processing operations carried out can be classified as necessary, appropriate and proportionate and no relevant residual risks to the freedoms and rights of the data

subjects have been identified following the implementation of all the mitigation measures identified in the above assessment.

As a result, it is not deemed necessary to initiate a prior consultation procedure under article 36.1 of the GDPR.

10. Engagement with supervisory authorities

Firstly, it should be noted that the development of the pilot has been led by VSSL, which has initiated and maintained contacts regarding TrustPid with relevant data protection supervisory authorities in the spirit of transparency and with the aim of cooperating with said authorities to guarantee full compliance with the data protection obligations.

In this regard, in the case of the German pilot, VSSL decided to make an informal approach to the German supervisory authority (BfDI) during the summer of 2021. After several interactions with BfDI, the main findings and recommendations obtained were incorporated into the project. In summary, they are as follows:

- Validation of the delegated consent approach through the advertisers' and publishers' CMPs[3];
- A requirement to obtain consent for TrustPid regardless of other purposes, by means of a dedicated TrustPid pop-up separate from the main Brands and Media CMP that allows the user to reject it with a single click;
- Validation of an approach to data assignments between independent data controllers, although the model should be adapted to move towards a co-responsibility model in the future.
- The leading data protection authority will likely be the authority of the country in which the future JV is incorporated. In Germany, BfDI's responsibility is the processing taking place at the telcos.

In addition, the CNIL, ICO, and AEPD have also been engaged.

[3] A CMP (Consent Management Platform) is a technological tool tasked with collecting and storing the information on the consents of the visitors to the website who have authorised the advertiser to use them in a particular way. In addition, the platform is responsible for transmitting the consents to all the advertiser's partners upon request.

ANNEX I: PRIVACY USER EXPERIENCE

Telco network and service previously blocked

Network of other Telcos outside the pilot