Data Protection Impact Assessment

Procedure

IDCo / TMI / Argus / TrustPid

A consent-based platform to create unique network-based IDs for internet users that can be used to provide a personalised online experience (including advertising, personalised content and product recommendations or to perform analytics)

Version 1.6
15 02 2023

NOTE: This document is currently being updated due to ongoing regulatory engagement with data protection regulators in Germany, France, UK and Spain and is therefore subject to change.

Please also note that this document seeks to cover the current implementation of the solution as part of the MVP and is therefore subject to change for future iterations.

Confidential business and operating information

Content

1. Documentation of the Data Protection Impact Assessment for this process

Implementation accountability		
Who has direct responsibility for the process defined in Art. 35 (1) GDPR and therefore the implementation of this data protection impact assessment?		
1.1	Controller	Vodafone Sales and Services Limited, Vodafone House The Connection Newbury, RG14 2FN England (VSSL), is the responsible controller for this DPIA, and delivers the TrustPid service during the pilot stage. Above role will be transferred to an EU based Joint-Venture, based in Belgium, once the pilot ends. NOTE: TrustPid requires data processing by multiple parties with different roles in the processing. These parties include the participating mobile network operators (Telco) to whose customers advertising is displayed when they visit a participating Publishers' websites (after they have given their consent), Publishers who maintain websites on which consents are gathered and advertising displayed, as well as Advertisers who choose what ads are displayed on Publishers' websites. Taking into account the complexity that arises from the involvement of multiple parties, with the aim of maintaining a coordination that helps the understanding of the project and its comprehension from a data protection point of view by the different control authorities consulted formally or informally or requiring access to this DPIA, VSSL maintains the overall and unique DPIA for the project, and the outcomes will be applied to the project as a whole. In this regard, each party has participated in the review of this DPIA. This does not prevent them from being able to conduct their own, additional DPIAs, if deemed necessary.
1.2	Department (s)	Group Commercial, Vodafone Group Services
1.3	Business owner (name)	Nikos Vlachopoulos

2. Description of the processing operations in terms of their necessity and proportionality in relation to the purposes

Processing operation or pooled processing operations		
2.1	Title	TrustPid (or project Argus or TMI or IDCo; terms used interchangeably in this document and/or used in a public manner) is a consent-based platform that creates unique network-based IDs for internet users that can be used to provide a personalised online experience (including advertising and personalised content and product recommendations or to perform analytics). This DPIA covers the service as a whole, focusing on the targeted advertising use case being trialled as part of the MVP. Other use cases will be addressed as and when required.
2.2	Description	TrustPid is a solution designed to enable online advertising activities in a more secure, controlled, and transparent way compared to the third-party cookie-based model way, whilst bringing enhanced choice and control to individuals over the processing of their data in the advertising ecosystem. TrustPid is a value-added service provided in conjunction with Telcos, whereby the value or added benefit provided to users is empowerment or enhanced control and transparency regarding the use of their data in the context of online advertising. Specifically, TrustPid service provides centralised consent management for users enabled via IP address identification by Telcos in their network. In contrast to today's advertising ecosystem where users frequently are not aware of who has their data and have limited power to restrict its spread amongst intermediaries in the sector, TrustPid delivers a controlled ecosystem in which the distribution of a user's data is limited only to those parties that have a direct contractual agreement and clear consent and only with the minimum data required, as well as crucially enabling users to self-serve and manage their consents across all websites visited (participating in the trial) in a single platform. [redacted] No identifiers are created unless the user has given her/his voluntary, informed, specific and revocable opt-in consent on the advertiser and publisher's website. To reduce the risk of cross site tracking and uncontrolled data sharing and profiling, the solution provides a controlled ecosystem underpinned by direct contractual relationships with all parties involved in the data processing/sharing and relying on first party IDs rather than third party. [redacted] In doing so, the data processing is minimised as third parties in the ad ecosystem (demand and supply side platforms) only have access to randomised tokens. These tokens do not directly identify data subjects and are not identifiable data to them.

(1) Different IDs are used for different purposes, and they are generated in a way that prevents backwards direct re-identification. [redacted]

(2) [redacted]

(3) [redacted]

The solution also involves a robust transparency and consent experience. The solution operates a delegated consent model, whereby consent is given on the advertiser and publisher's website to cover the entire TrustPid ecosystem (all processing activities undertaken by each party (Telco, Advertiser/Publisher, VSSL) in scope to deliver the service). The solution does not rely on a "global consent", instead it requires consent to be collected for each participating website i.e., one consent obtained on one website will not activate TrustPid on all its partner websites. [redacted]

To ensure the validity and quality of consent obtained on participating websites, specific consent requirements are established in the contract with participating parties which define the consent form/design and text that must be implemented by the same. The consent text for TrustPid, defined by VSSL in consultation with the participating Telcos, covers:

(1) [redacted]

(2) Onwards processing by TrustPid platform managed by VSSL to generate additional randomised IDs [redacted], MarTech ID and AdTech ID) [redacted] (MarTech ID and AdTech ID) to profile and deliver personalised content, products, offers or advertising to the user (Article 6(1)(a) GDPR)

(3) Placing and accessing of IDs (MarTech ID and AdTech ID) and related cookie [redacted] on the user's device (Article 5(3) ePrivacy Directive)

To increase transparency and user control, the service provides a self-serve one-stop-shop dedicated site ("the Privacy Portal") which enables individuals to control their consent. Specifically, users are able to find detailed information about the service, view the privacy statement and exercise their data subject rights including immediate access to data (view in one place all sites to which they have consented to receive a personalised experience based on the network-based solution) as well as review consents given and manage preferences easily in one place, including consent revocation either per site or on a blanket basis, or to block the service entirely.

[redacted]

		[redacted]
2.3	Purpose	(1) Enable advertisers and publishers to profile and provide users with a personalised online experience in such websites (including advertising and personalised content and product recommendations or to perform analytics). (2) Provide a value-added service to users where the added benefit is provided by leveraging network based IDs to enable centralised management of consents, empowering users regarding the use of their data in the context of online advertising. Specifically, a self-serve centralised permissions management platform is provided for users to stay in control of the processing of their data via the network-based solution by enabling them to manage their preferences and exercise their data subject rights at any time.
2.4	Lawful basis for processing	The processing is based on: • Article 6(3) of the ePrivacy Directive - Consent collected for a value-added service involving the processing of user's IP address [redacted] • Article 6(1)(a) GDPR – Consent to cover onwards processing by TrustPid platform managed by VSSL [redacted] To enable the user to effectively manage their consents through the centralised permission management platform. • Article 5(3) of ePrivacy Directive – Consent to store and access IDs (MarTech ID and AdTech ID) and related cookie [redacted] on the user's device to deliver the TrustPid service. Storage and access of cookie [redacted] which stores consent status given by user for the TrustPid service is strictly necessary to provide the service requested by the user. See Annex 5 for specific details on cookies used under TrustPid Cookie Policy. • Article 5(3) of ePrivacy Directive - Necessary to process users' IP addresses for the purpose of determining if a user is eligible to use the TrustPid service and identify [redacted] (2) verify the user to determine eligibility to access the Privacy Portal. [redacted] The conditions for consent are fulfilled (Article 7 GDPR): 1. **Freely given** - Real choice provided with no repercussions i.e., one click reject button available 2. **Specific -** [redacted] 3. **Informed** - All parties involved identified along with their respective processing activities undertaken as part of delivering the TrustPid service 4. **Unambiguous** - Effect of granting consent specified i.e. activates the TrustPid service to show personalised advertising

		5. **Revocable** - Transparency provided around options available to manage and/or revoke consent
2.5	Are the purposes for processing clearly defined, legitimate and transparent?	☒ Yes **Clearly defined:** • The purposes are clearly stated in the permission that the user needs to provide on both 'market sides', i.e., to brands and publishers. Specifically, the consent covers VSSL, user's network operator and website operator's (advertisers and/or publishers the user has visited) processing of user's data for the purpose of: ○ Activating the TrustPid service, including creating and managing user IDs [redacted] MarTech ID, AdTech ID) and sharing these with advertisers and publishers (and other third parties acting on our or their behalf) to provide the user with a personalised online experience in websites visited (including advertising and personalised content and product recommendations or to perform analytics); ○ Storing and accessing the MarTech ID, AdTech ID created on user's devices; as well as ○ Providing users with a centralised self-serve platform to manage their preferences and exercise their rights. **Legitimate:** The TrustPid s solution is a novel way of doing digital advertising, designed to address many privacy challenges in the current cookie-based online advertising ecosystem through a "privacy first" approach. The solution has a strong focus on transparency, consent and control, data minimisation, accountability, and compliance. The ability to identify users across websites is crucial for Publishers and Advertisers' commercial success, however the current digital advertising model enables the collection, distribution and use of data at scale without sufficient safeguards to protect users' digital rights. In contrast, TrustPid intends to deliver a privacy-led network-based solution which will allow users enhanced transparency and control over their data, while enabling advertisers and publishers to optimise their online content and display advertising activities. **Transparent:** Transparency at first point of contact in permissions text (consent pop-up): • The TrustPid Privacy notice is available to the user via hyperlink within the permission text. A Privacy Portal can also be accessed by the user within the permission text, which includes additional information on TrustPid, contains the privacy notice and enables the user to track and manage the consents provided to the brands and publishers, including a blacklist option which, when selected, means that the user is opted-out from all brands and publishers. Transparency in TrustPid Privacy Portal: • The information provided in the TrustPid Privacy Portal covers the following: (1) Information about the TrustPid service, including objective, how the technology works and conditions for activation. Specifically, users are informed that the service operates only on the basis of user's explicit consent and not active by default, consent is revocable in multiple ways as well as can be entirely suspended by applying a block. See Annex 4 for user journeys.

		(2) Clear activation status – [redacted] (3) Privacy Notice – The TrustPid Privacy Notice is available in the native language of each market where the Pilot is planned. The user will be presented with the portal including the privacy notice in the language of the country where they are browsing from. The user has the ability to switch languages using a feature in the top right corner of the TrustPid website. See Annex 5 for the latest version of the TrustPid Privacy Notice. Please note that French versions are currently being translated. Transparency in partner's sites: • Information about TrustPid is also included in all partner's sites (Telcos, Publishers and Advertisers) either via: (1) Partner's privacy statement – partners make reference to TrustPid in their own privacy statements or transparency centres which includes additional explanation of the TrustPid service and how to revoke consent which is either facilitated by providing hyperlinks to access directly the TrustPid Privacy Portal [redacted] (2) Hyperlink at footer of partner's website – partners insert a hyperlink accessible from footer of their websites specifically for TrustPid which when accessed by user it provides additional information about the service and option to amend consent. ☐ No Reason:_____

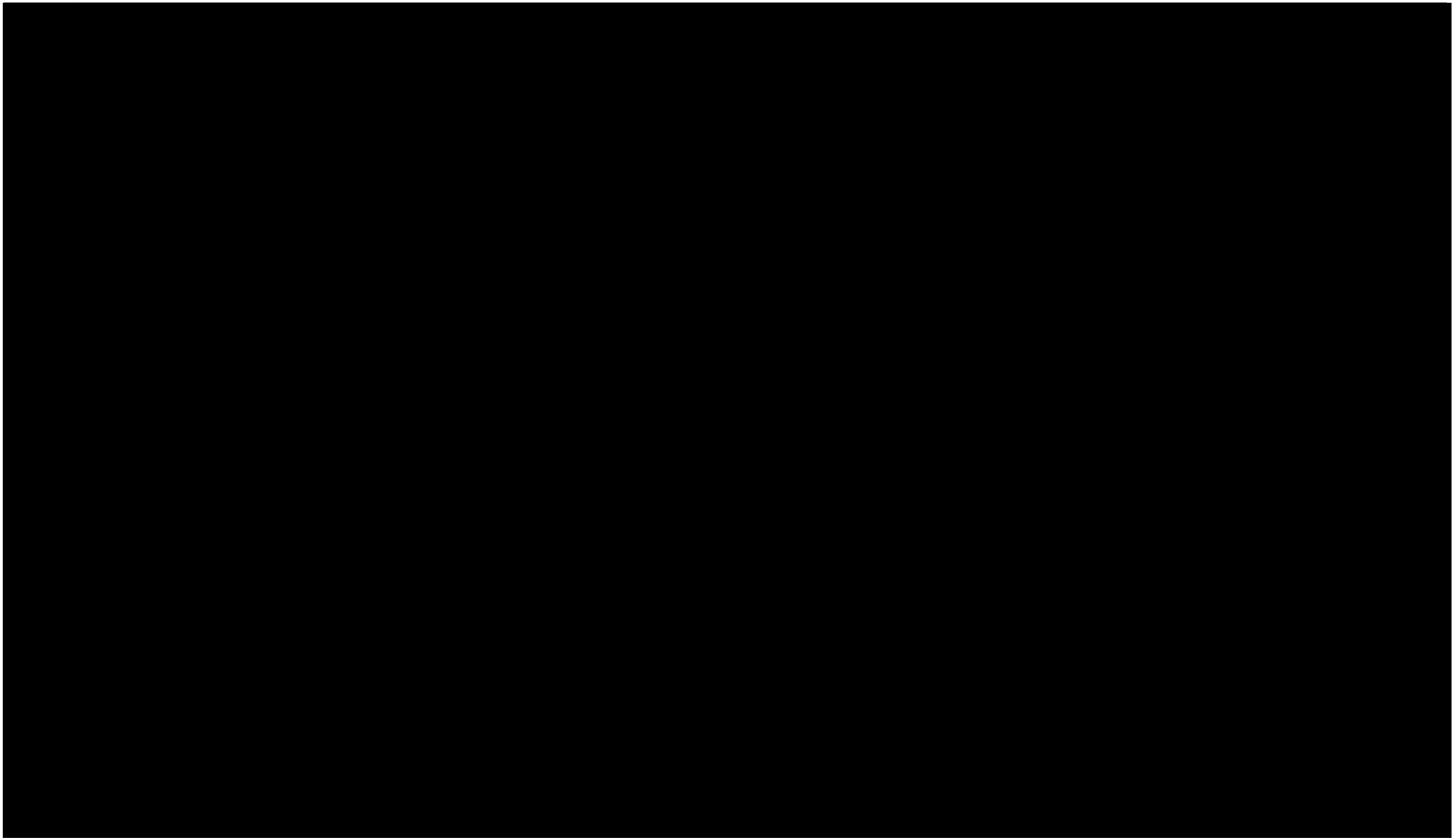
Data flows

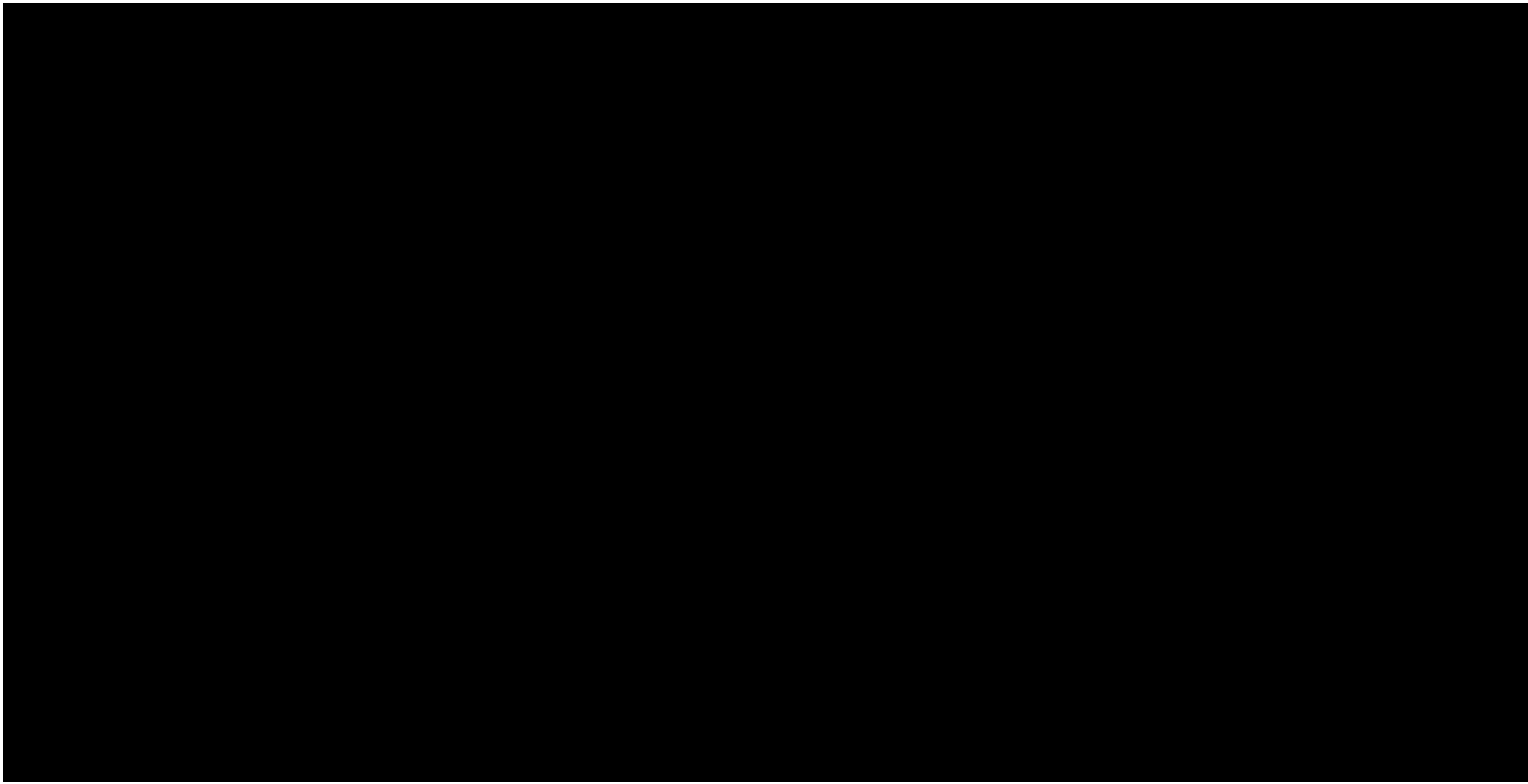
Provide a flow chart or written description of how the data are processed and, where appropriate, additional information or graphical representations to substantiate the description. The description must show:

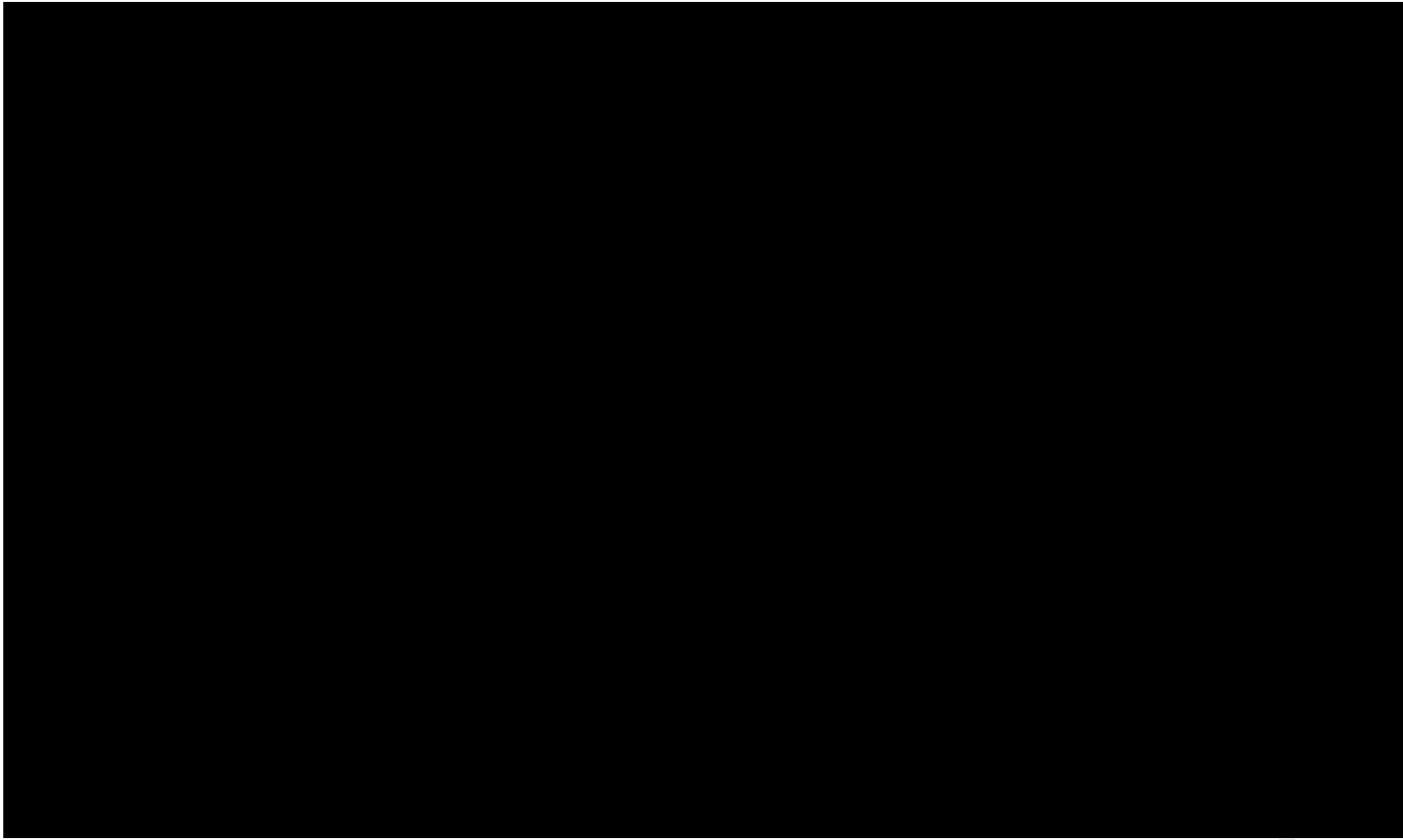
- the systems involved in the processing
- the systems from which the data are obtained
- the output format and recipients
- the technical object of processing
- the norms and standards, if any, which apply to the processing

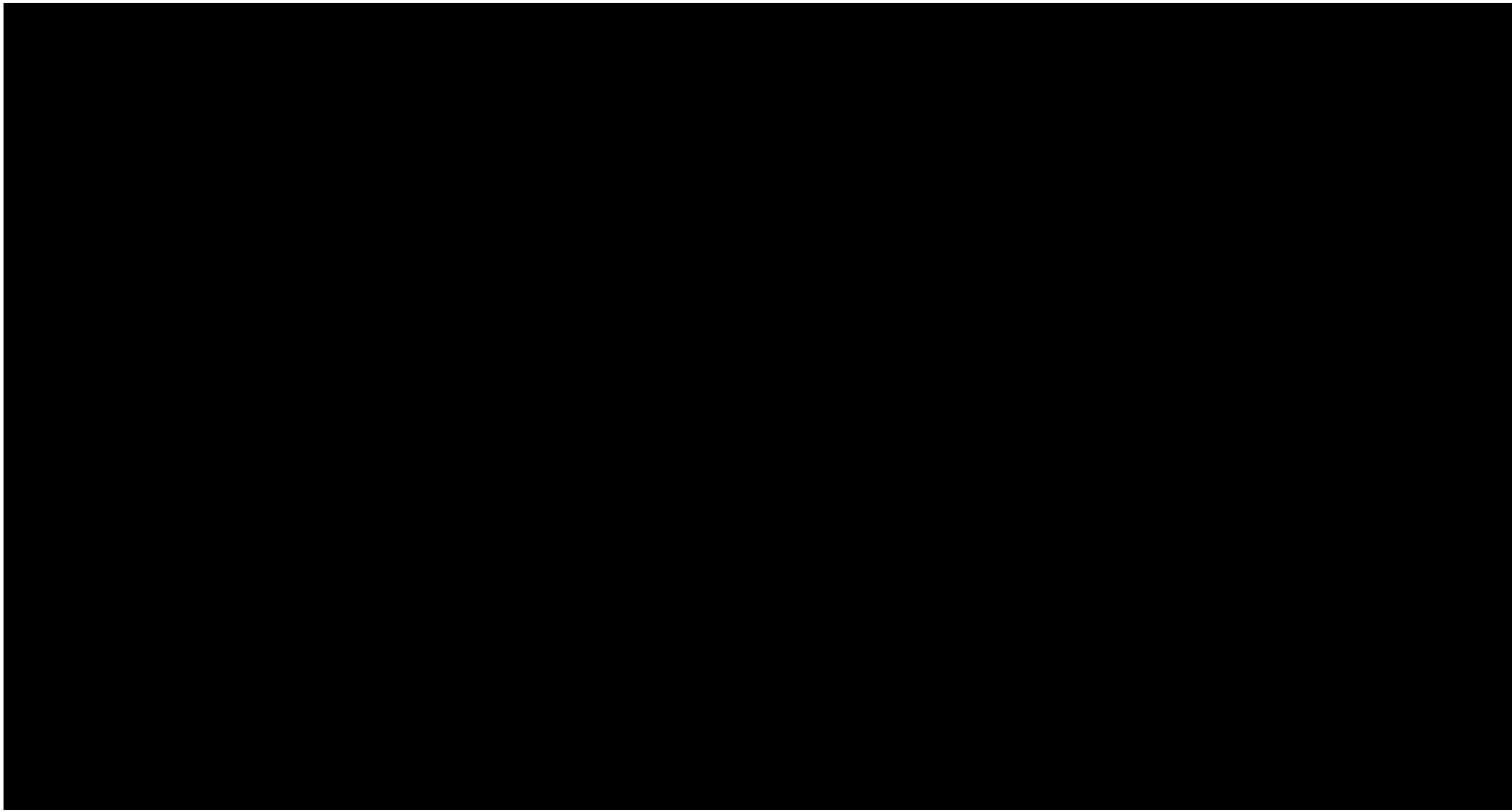
A description which is as detailed as possible will ensure traceability and reproducibility in the further assessment process. Relevant design documents can be appended to the DPIA as supporting information.

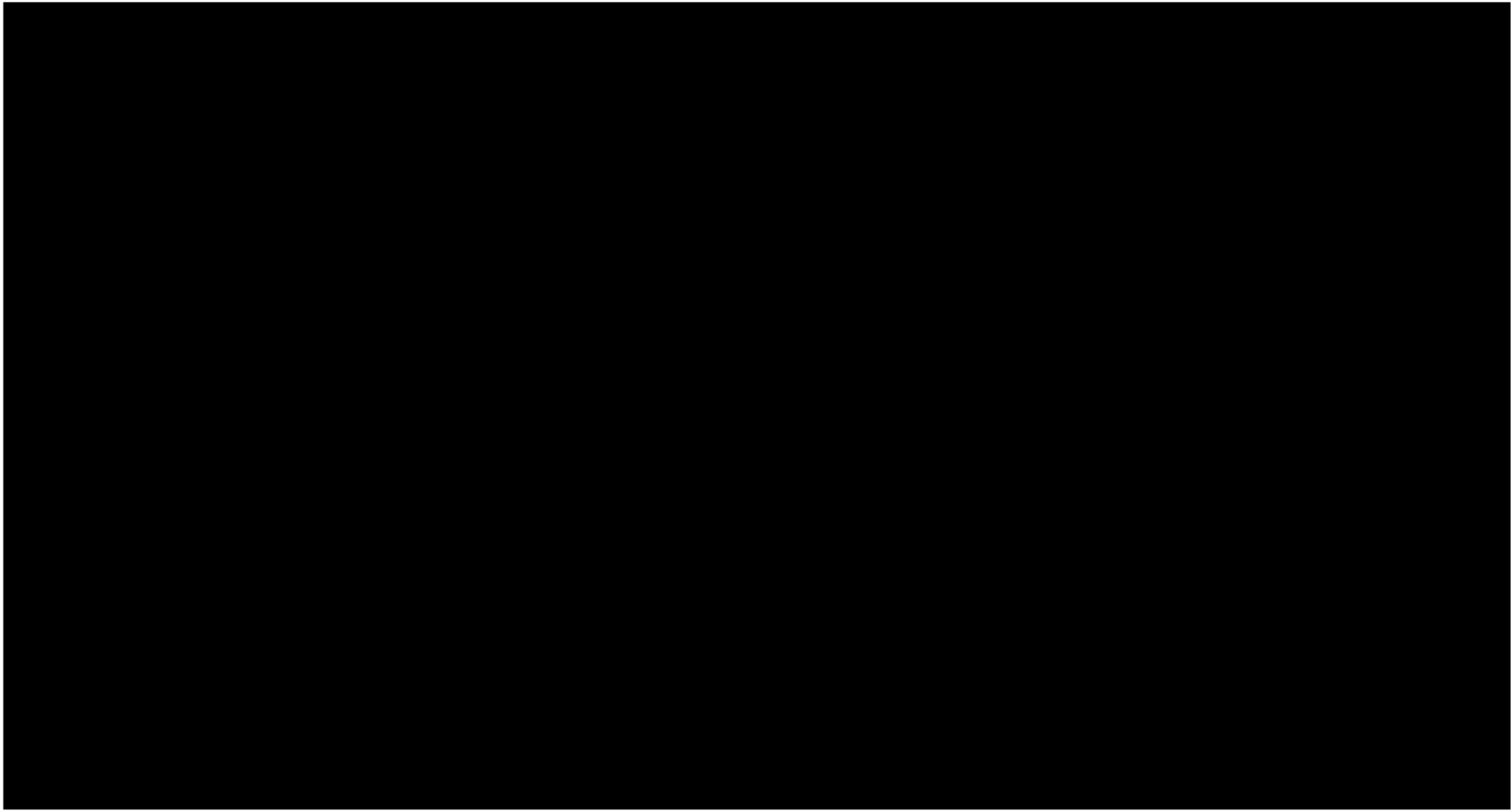
[redacted]





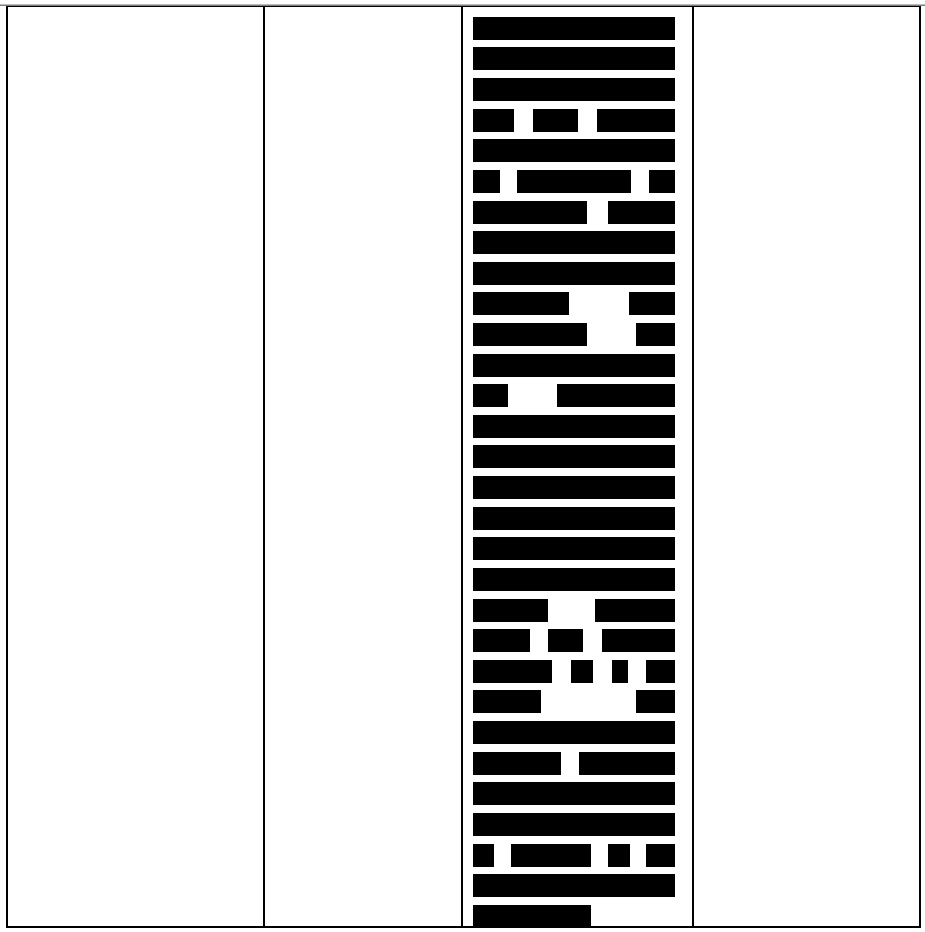






Classification of data categories, categories of data subjects, recipients and legal bases					
2.11	Data categories	**Master data** ☐ Name, surname (with title if applicable) ☐ (Postal) address ☐ Telephone number(s) ☐ E-mail address ☐ Date of birth ☐ Customer number ☐ Nationality ☐ Bank details ☐ Usernames ☐ ID card data ☒ Identifier /ID ☐ Password	**Service request data** ☐ Service request no. ☐ Installation date ☐ Options ☐ Service history ☐ Service deployment ☐ Products ☐ Discounts / campaigns/ promotions	**Contract data** ☐ Term ☐ Prices ☐ Credit rating information ☐ Hardware information ☐ Payment information ☐ Contract history ☐ Property information ☐ Contract start and end dates ☐ Products ☐ Active products/ tariffs ☐ Former products/ tariffs ☐ Aggregated usage information ☐ Cancellation reason ☐ IDs / references	**Transaction data** ☐ Working hours ☐ E-mails (content, logging) ☐ Log files ☐ Data on usage as per TMG ☐ Usage notifications ☒ Traffic data ☐ Video images ☐ Voice records ☐ Location data
2.12		[redacted]			
2.13	Category/categories of data subjects	☐ Customer family members/ contacts/ carers or similar ☐ Job applicants ☐ Former customers ☐ Former employees ☐ Management employees ☐ Business partners/ contractors ☐ Call participants/ other parties in telecommunications ☐ Leads/ potential customers ☒ Internet users ☒ Customers ☐ Suppliers ☐ External personnel ☐ Internal personnel ☐ Employees of other group companies ☐ Sponsors ☐ Sales partners			

		☐ Advertising recipients and rejecters ☐ Children ☐ Other: • N/A
2.14	Recipients	☐ Internal departments as per the process chart ☐ Other internal departments: [please specify] ☐ Sales partners ☒ Technical service partners ☐ Marketing: agencies, lettershops etc. ☐ Public authorities ☒ Other external bodies: • Telcos, Brands, Publishers, and AdTech Vendors (DSP, SSP)
2.15	Processors	☒ Yes, as follows: [redacted]

		[redacted]  ☐ No
2.16	Sub-Processors	[redacted]  ☐ No
2.17	Transfer to third countries	☐ No ☒ Yes – secure country outside the European Union with EU adequacy decision: • [redacted]

		[redacted] ☐ Yes, other countries
2.18	Erasure deadline What is the lifecycle of data and processes?	Retention periods are specifically defined per ID [redacted] See Annex 2 for detailed retention information.
2.19	Technical and organisational measures (TOMs)	☐ No special TOMs are implemented ☒ The following TOMs are implemented for data processing: [redacted]

[redacted]

<table>
<tr><td></td><td></td><td>• [redacted]</td></tr>
<tr><td>2.20</td><td>Proportionality</td><td>The invasion of privacy is proportionate in relation to the purpose.
The processing is necessary to achieve the objectives.
An alternative procedure, which would prejudice the data subjects' rights and freedoms to a lesser extent, is not available.
The collected data are required, relevant and restricted to the amount necessary for processing.

<u>Proportionality test of processing operations</u>

In order to check whether a processing operation is a measure restricting a fundamental right, this operation has to pass the three points of the so-called proportionality test

<table><tr><td>Judgement of appropriateness: the means must be suitable or the processing must be suitable for the achievement of the proposed purposes.

(Assess whether the activity carried out is adequate to achieve the intended purpose).</td><td>TrustPid is the European telecommunications industry's bid to solve two main problems:

1. Offer an alternative to third-party cookie-based identification services, which are expected to disappear completely by 2023; and
2. Providing technology that gives users greater control over their online privacy preferences by enabling control of these preferences in a single privacy portal.

TrustPid is expected to enable use cases with high commercial value in terms of personalised advertising and content, allowing the European industry to compete with other giants such as Google or Meta.

The aim of the pilot is to confirm whether these estimates are correct before moving to a future commercial phase.

The first use case is that of retargeting, which will allow advertisers:

- Better understand the users accessing their websites (profiling); and
-Offer your users personalised advertising in online media in a more efficient way and avoid repetitive impacts.

[redacted]

On the basis of the above, it can be concluded that TrustPid will be a suitable means to achieve the objective pursued.</td></tr><tr><td>Judgment of necessity: the processing</td><td>There are similar alternative mechanisms to Telco that</td></tr></table></td></tr>
</table>

			must be the only one capable of achieving the intended purpose in such a way that there is no other means of achieving that purpose in a less burdensome way for the data subject. (Assess whether there is a less invasive or equivalent mechanism to the one proposed for achieving the intended purpose or whether it can be achieved by means of another more moderate and less privacy-intrusive activity).	are already in place, such as all those relating to the online advertising industry using cookies and similar technologies andcommon frameworks such as the IAB's TCF 2.0. However, these mechanisms are considered more invasive of user privacy as they allow exhaustive user tracking in different online web and app environments through a multitude of technologies that overlap and are used jointly, in an environmentpractically dominated by large non-European ***players*** that maintain control over the entire advertising chain, an industry called into question by European control authorities, which runs the risk of disappearing or being subject to greater control by these ***players*** once third-party cookies disappear and which, moreover, does not allow quality identification of the user in online environments. In view of this, the emergence of alternatives such as TrustPid, led by European players and with Privacy projected from the design and by default of the solution, is necessary. **TrustPid Privacy Principles** - Data minimisation: • Separate and independent IDs for each brand (no ability to create a complete picture of users'browsing habits). • MarTechIDs expire after 90 days. • [redacted] • Pseudonymised identifiers (not containing direct identifiers) are always used. - Prohibition of special categories: • Prohibition to infer or process special categoriesof data. • VSSL / JV do not profile users nor do they knowtheir browsing habits. - Default consent: • The only legitimate basis is consent. • [redacted] • Denial of consent at a click. • [redacted] • Centralised privacy portal with the possibility torefuse all consents granted on blanked basis. • Access to the privacy portal from brand and media websites. - Transparent layered information: • Layered informed consent. • additional information to its customers through its channels. • Use of plain and transparent language. - Contractual safeguards for stakeholders:

				• TrustPid IDs can only be used for specific purposes, without the possibility of further processing. • Prohibition to reverse the pseudonymisation process. • Obligation to comply with the TrustPid consent standard. • [redacted] - Privacy as a value proposition: • Privacy at TrustPid is not mere regulatory compliance, but part of the value proposition tocompete. • TrustPid has in its roadmap to improve current privacy functionalities and to use its technology to solve Internet privacy challenges. In view of the above, it can be concluded that TrustPid is a necessary solution to achieve a fairer and more privacy-friendly online advertising industry, a solution led by European players as opposed to an existing alternative that does not have Privacy as abasic principle configured from the design of the solution.
			Strict proportionality test: analysing whether the impact on privacy is reasonable in relation to the objective pursued by the purpose of the processing. (Assess whether the impact of the processing on the privacy of individuals is proportionate and balanced against the benefit I derive).	The solution is based, from start to finish, on the use of pseudonymised identifiers of a user who has expressly consented to their use with the aim of developing online advertising use cases that can benefit them by showing them personalised advertising that is truly relevant and of interest to them. Telcos will only process data relating to their customers. VSSL will carry out all processing in accordance with Art. 11 [redacted] Consequently, the impact on user privacy is considered to be proportionate to the intended purpose of TrustPid.
			Conclusion	Having assessed all the above points, it can be concluded that TrustPid's processing passes the triple test of appropriateness, necessity and proportionality, without prejudice to the mitigating measures that need to be put in place to reduce the existing risks, as described below.

Measures to protect the data subjects' privacy rights have been taken.		
2.21	How have the data subjects been informed about the processing of their personal data?	[redacted]

		[redacted] (2) Via TrustPid Privacy Portal which includes detailed information about the TrustPid service, its objectives and features as well as detailed information on the processing within the TrustPid Privacy Policy in line with Article 13 GDPR. See Annex 4 for user journeys of the Privacy Portal. (3) Via the participating partner websites: • Telcos' websites - Participating Telcos include information on TrustPid service in their Privacy Policies or transparency centres within their websites. Example below: "You can manage your settings and preferences at any time via the data protection portal at www.trustpid.com For more information, visit the TrustPid official site at www.trustpid.com" • Publisher/Advertisers' websites – Participating website operators include reference to TrustPid in their own privacy policies which includes additional explanation of the TrustPid service and how to revoke consent which is either facilitated by providing hyperlinks to access directly the TrustPid Privacy Portal [redacted] o amend their preferences.
2.22	If applicable – how was the consent of the data subjects obtained?	The consent is collected via participating advertisers' and publishers' websites (See Section 2.10 above for detailed consent user experience and technical flow, and Annex 6 for consent guidance). Users need to provide their consent on every website individually for the processing to take place and to enable generation of IDs by the TrustPid platform. This means that there is no "global consent" applicable to TrustPid, instead the solution has also been designed in a way which requires consent to be gathered for each specific domain that the user visits.
2.23	How can the data subjects exercise their rights?	The TrustPid solution has been designed to provide a self-serve one-stop-shop portal to enable users to manage their preferences and exercise their data subject rights at any time. See Annex 3 for detailed description on exercise of rights.
2.24	Are the processor's obligations clearly defined and contractually agreed?	☒ Yes See Section 2.19 above for details on contractual set-up. In respect of sub-processors, contractual agreements concluded with Processors require them to set up legally binding terms with such sub-processors to ensure the same obligations imposed on the processor with regards to the data processing flow down to them. ☐ No

3. Relevance check

Review of inclusion criteria	Yes	No
A data protection impact assessment must be carried out if the answer to at least one of the following is "yes".		
Is the process on the list (blacklist) of processing operations which are subject to the requirement of a DPIA? (Art. 35 (4) GDPR)	☐	☒
Is a systematic and extensive evaluation of personal aspects relating to natural persons and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person carried out? (Art. 35 (3) a GDPR)	☐	☒
Are special categories of personal data processed on a large scale? (Art. 35 (3) b GDPR)	☐	☒
Does the systematic monitoring of publicly accessible areas take place on a large scale? (Art. 35 (3) c GDPR)	☐	☒

Risk assessment	Yes	No
If none of the inclusion criteria apply, it is necessary to assess whether the processing operations are likely to be associated with a high risk1. This is the case if two or more of the following criteria apply:		
Evaluation and scoring of personal data (including profiling and predictive models, or behaviour or marketing profiles)	☒	☐
Automated decision-making with legal or other similarly significant effects	☐	☒
Systematic surveillance, with the objectives of observation, monitoring or control	☐	☒
Confidential data or special categories of personal data pursuant to (Art. 9 and 10 GDPR)	☐	☒
Data processing on a large scale (number of data subjects, volume of data, duration and permanence, geographic scale)	☒	☐
Comparison or combination of data records	☒	☐
Data pertaining to vulnerable data subjects (recital 75 GDPR)	☐	☒
Innovative use or application of new technological or organisational solutions (e.g., fingerprint and facial recognition)	☐	☒
Processing which prevents the data subject from exercising a right or using a service/ executing a contract	☐	☒

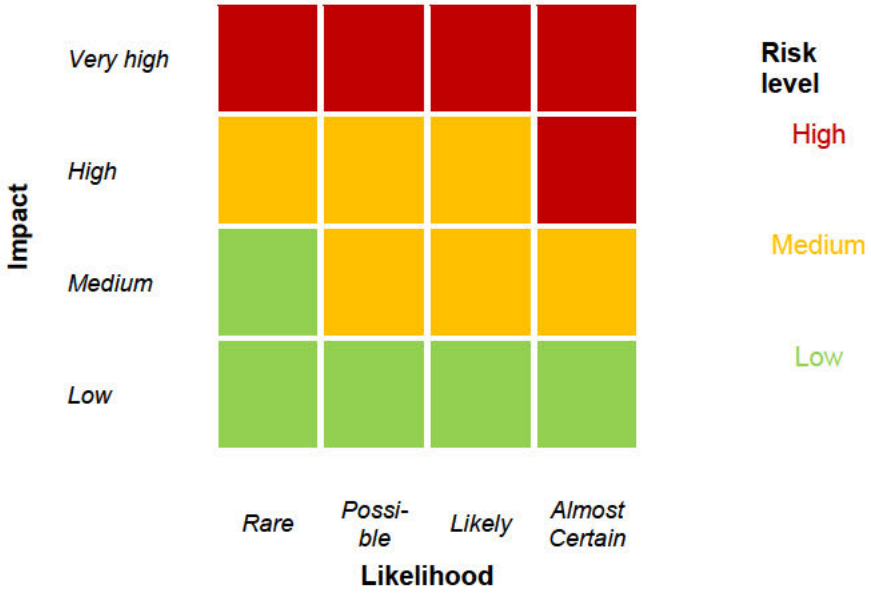
Results of the impact assessment:
With regard to the processing operations covered in this document a DPIA is ☒ necessary, because an inclusion criterion applies, or they are likely to be associated with a high risk for the rights and freedoms of the data subjects. ☐ not necessary.
State the reasons why the DPIA is not necessary.
N/A

[1] The processing operations are reviewed to establish risk potential on the basis of the criteria published by the Article 29 Data Protection Working Party (WP 248, version 1)).

4. Risk determination and measures

1. Classification methods

Risks are determined in accordance with the methods for risk identification set out in the internal Privacy Risk Management policy. The total risk is evaluated on the basis of the graphic below (further information can be found in the policy, particularly page 13 ff and page 33 f of version 1.1 dated 13.9.2019).



2. Risk sources

The following overviews include the relevant risks for the process being assessed. They include any technical risks, risks to data integrity, risks relating to the confidentiality of information and risks for the data subjects. In the latter risk group, the Vodafone "Human Impact Analysis" process is used to systematically assess the immaterial and material risks for data subjects. Identified risks are mitigated by way of measures (particularly technical and organisational measures) or by adapting the processing operation. This, and any remaining high residual risk, are documented.

Inherent risks of ads ecosystem and TrustPid measures identified to address the risks			
Category	**Risk**	**Measures implemented**	**High residual risk?**
Inadequate lawful basis	a) Lack of robust consent to comply with e-privacy laws to use tracking technologies b) Balancing exercise when relying on legitimate business interests as the lawful basis lacking	• Only consent will be relied on to cover the tracking technologies aspect of the processing, including one-click reject option for users to deny consent to TrustPid service •	No
Lack of adequate technical and organisational measures	Inconsistent technical and organisational security measures applied to adequately secure data shared within ads ecosystem in transit and rest	• [redacted] • Data protection agreements in place with entities involved defining permitted uses of data shared. • TrustPid Platform incorporates technical and organisational security measures: • Recurring employee training (e.g., data protection and security trainings) [redacted]	No
Incompetent processing	a) Incorrect or inappropriate profiling b) Processing which makes systematic monitoring possible	[redacted]	No
Uncontrolled data processing/sharing and insufficient transparency of processing	a) Number of parties in ads ecosystem and data shared amongst them leads to an uncontrolled data sharing b) Large scale processing and data sharing undertaken without users' full knowledge	• [redacted] •	No

		Specifically, the privacy portal is a self-serve centralised permissions management service provided to user which enables them to view list of sites – parties processing their data - which they have provided consent to use TrustPid service as well as amend their preferences against the same. [redacted]	

Relevant risks for TrustPid and measures to reduce the risks					
Category	**Risk**	**Impact**	**Likelihood**	**Corrective measures**	**High residual risk?**
Integrity and confidentiality of data	Due to the technical conditions of the MVP operation of the solution, there is a risk that user data stored and made available to user within the TrustPid Privacy Portal (under "Manage Preferences" section) can be accessed and managed by other users if they share their hotspot/tethering connection as they would be sharing the same connection and therefore be verifies as same user by the service.	Medium	Likely	This risk will be mitigated by: [redacted]	No
Misuse of data	There is a risk that the Demand Side Platforms (DSPs) [redacted]	High	Possible	This risk will be mitigated by: [redacted]	No

				[redacted]		

Other risks considered						
Category	**Risk**	**Examples**	**Impact**	**Likeli-hood**	**Corrective measures**	**High residual risk?**
Risks to confidentiality						
			Immaterial risks			
Negligence	a) Unintentional human error	1) Non-compliance with security instruc-tions, 2) disclo-sure of IDs and passwords, ac-cess permis-sions, 3) incor-rect administra-tion of systems and applica-tions, operation of systems and applications, 4) Incor-rect disposal of data storage media, 5) insecure storage of mo-bile computers, loss of confi-dentiality or	Medium	Rare	• [redacted]	No

		integrity due to negligence				
Manipulation Reconfiguration	a) Manipulation of hardware and software b) Software vulnerabilities or errors	1) Changes to data links 2) Use of known vulnerabilities to retain or intercept data 3) Changes to the target system	Medium	Rare	• See technical and organizational measures and state of the art security measures • [redacted]	No
Theft Fraudulent use	a) Unauthorised access to IT systems b) Fraudulent use of personal data c) Loss of customer data	1) Theft of hardware or data storage media 2) Use of a third party account 3) Extraction of personal data 4) Transfer of data to an unsecure data storage medium	High	Rare	• See technical and organizational measures and state of the art security measures [redacted]	No
Risks for the data subjects						
Material risks						
Identity theft	a) Ability to log into other, non-Vodafone services with username password combinations - enables one or more of the below harms	1) Unauthorised access to email and password combinations 2) Unauthorised disclosure of bank account numbers, sort codes, home address, real names and	High	Rare	[redacted]	No

		other such information Unauthorised disclosure of security questions (e.g. answers to questions such as mother's maiden name)				
Death bodily harm other risk to personal safety	a) Bodily attack (e.g. jealousy or politically motivated)	1) Unauthorised disclosure of location data, in particular if enables ongoing monitoring, or reveals home location; 2) Unauthorised disclosure of communications content or traffic data Unauthorised disclosure of private phone numbers or home address (e.g. when under restraining order)	Very High	Rare	[redacted]	No
	a) Stalking of an individual. b) Ongoing monitoring of an individual	1) Unauthorised disclosure of location data, in particular if it enables ongoing monitoring, or reveals home location (e.g. when under restraining order);	Medium	Rare	[redacted]	No

		2) Unauthorised disclosure of communications content or traffic data Unauthorised disclosure of private phone numbers or home address (e.g. when under restraining order)				
	a) Harm to medical health	1) Tampering with accuracy of personal data, leading to an incorrect assessment of medical health; Prescription misuse / fraud as a result of access to information which enables identity theft.	Very High	n.a.		
Loss of freedom	a) Incarceration / criminal conviction of the wrong individual;	1) Unauthorised access to data that enables full identity theft; Unauthorised access to CRM/billing systems resulting in the wrong persons being convicted of fraud or other offences.	Medium	n.a.		

Property/assets harm	a) Burglary / theft of property	1) Unauthorised disclosure of location data, in particular if it enables ongoing monitoring, or reveals home location; 2) Disclosure of present location, revealing that home / other property is unattended; Unauthorised disclosure of private phone numbers or home address	Medium	Rare	[redacted]	No
Monetary Loss Financial Fraud	a) Credit / payment card fraud; b) Access to bank accounts, ability to make unauthorised money transfers; c) Sale of assets; similar other loss of assets; d) Accrual of debt in another person's name.	1) Unauthorised disclosure of credit card details (consider if full / partial details have been disclosed); 2) Unauthorised disclosure of bank account numbers, sort codes, home address, real names and other such information Unauthorised disclosure of security questions (e.g. answers to questions such as mother's maiden name)	High	Rare	• There is a small risk that if someone access the list of websites visited on the privacy portal that they may try and use that to create a profile of the individual for impersonation fraud. [redacted]	No

Monetary Loss Financial Fraud	a) Unauthorised changes to employment agreements, salary, pensions or other benefits; b) Sale of assets.	1) Unauthorised edit -access to HR administration systems; Unauthorised edit -access to MyHR.	Medium	n.a.	• No employee data involved	
Monetary Loss Financial Fraud	a) Unauthorised changes to customer contracts; b) Unauthorised tampering with CDRs / bills. c) directing customer payments to fraudulent accounts;	1) Unauthorised access to CRM systems (consumer / enterprise) Unauthorised access to network, mediation or billings systems, enabling changes to CDRs and billing records.	High	n.a.	• [redacted]	
Blocked / Differential Access to Credit/Loan	a) Accrual of unpaid debt in another person's name resulting in loss of credit scores b) Denying credit to all / some customers	1) Unauthorised disclosure of credit card details (consider if full / partial details have been disclosed); 2) Unauthorised disclosure of bank account numbers, sort codes, home address, real names and other such information 3) Unauthorised disclosure of security questions (e.g.	High	Rare	• Whilst brands and publishers may use the data to provide personalised marketing this profile should not be used for decision making purposes	No

		answers to questions such as mother's maiden name); Unauthorised edit -access to CRM systems;				
Negative impact on employment	a) Inadvertent resignations; b) Changes to performance records; c) Posing as another person, harassing others, sending inappropriate emails etc.	1) Unauthorised edit -access to HR administration systems; 2) Unauthorised edit -access to MyHR. Unauthorised access to email / skype / Workplace and other such systems posing as other users.	High	n.a.	• no employee data involved	
Negative impact on employment	a) Employment discrimination, e.g. based on gender, race, health data, sexual orientation, religious beliefs or other sensitive data	1) Unauthorised -access to HR administration systems; 2) Unauthorised -access to MyHR; 3) Unauthorised access to people survey data, in particular questions on sexual orientation; 4) Unauthorised access to email / skype / Workplace and other such	High	n.a.	• no employee data involved	

		systems posing as other users. 5) Unauthorised access to CRM systems (consumer / enterprise) Unauthorised access to network systems				
Loss of service **Denial of access to services**	a) Discontinuation / other disruptions of communications services to one or more customers / users	1) Unauthorised access to CRM systems (consumer / enterprise) Unauthorised access to network systems	Medium	Rare	• Adequate technical and organizational security measures will be in place to prevent cyber attacks to the TrustPid platform	No
Loss of service **Denial of access to services**	a) Denial of access to Vodafone communications / other publicly available services) b) Denial of post-paid service to all / some customers.	Unauthorised edit -access to CRM systems;	Low	Rare	• Adequate technical and organizational security measures will be in place to prevent cyber attacks to the TrustPid platform	No
Immaterial risks						
Damage to reputation / Embarrassment / emotional distress	a) Disclosure of race, health data, sexual orientation, religious beliefs, political convictions or other sensitive personal data; b) Disclosure of maternity leave / sick leave / disciplinary records; c) Disclosure of salary / pensions / other benefits; d) Disclosure of CDRs and/or communications content	1) Unauthorised -access to HR administration systems; 2) Unauthorised -access to MyHR; 3) Unauthorised access to people survey data, in particular questions on sexual orientation; 4) Unauthorised access	High	Rare	• No employee data involved • No sensitive data processed	No

		to email / skype / Workplace and other such systems posing as other users. 5) Unauthorised access to CRM systems (consumer / enterprise) Unauthorised access to network systems				
Damage to reputation / Embarrassment / emotional distress	a) Disclosing false/inaccurate personal data about an individual	1) Unauthorised edit – access to HR administration systems 2) Unauthorised edit -access to MyHR. 3) Unauthorised access to email / skype / Workplace and other such systems posing as other users. 4) Unauthorised access to CRM systems (consumer / enterprise) Unauthorised access to network systems	High	Rare	• There is a small risk that some brands and publishers may incorrectly profile individual based on their browsing behaviour or profile them on sensitive data types i.e. medical needs or sexuality.	No
Nuisance / Irritation	a) Increased nuisance calls b) Increased spamming	Unauthorised disclosure of private phone numbers, email addresses or home address (e.g. when	Low	Likely	• There may be a risk that users will be inundated with targeted advertising but the user will be able to opt out of this at anytime. In addition, TrustPid allows Brands to do frequency capping which can result in the targeting of less users.	No

		under restraining order)				
Verbal abuse	a) Disclosing sensitive information about someone, without their permission that could expose or subject them to verbal abuse: b) Harassment due to unauthorised disclosure of political opinion, or other sensitive personal data	1) Unauthorised edit -access to HR administration systems; 2) Unauthorised edit -access to MyHR. 3) Unauthorised access to email / skype / Workplace and other such systems posing as other users. 4) Unauthorised access to CRM systems (consumer / enterprise) Unauthorised access to network systems	High	Low	• There is a small risk that people within the same household may be able to see each others websites that have been consented to and may cause harm if the other household members use that data against the individual.	No
Loss of sense of personal security	a) Stalking of an individual. b)Ongoing monitoring of an individual	1) Unauthorised disclosure of location data, in particular if it enables ongoing monitoring, or reveals home location (e.g. when under restraining order); 2) Unauthorised disclosure of communications content or traffic data	Medium	Possible	• Whilst no traffic data or location data will be unauthorised disclosed, there is ongoing monitoring of the individual. This risk will be mitigated by asking for consent and allowing the user to opt out at any time.	No

		Unauthorised disclosure of private phone numbers or home address (e.g. when under restraining order)				
Loss of control over one's personality	a) Disclosure of data that allows persistent identity theft	1) Unauthorised disclosure of biometrical data (e.g. fingerprint, facial recognition algorithms) which allows recreation of a digital person. 2) Unauthorised access to CRM systems and contract data bases with signature data. 3) Unauthorised access to security questions.	Medium	n.a.		
Inability to exercise privacy rights	a) Disclosure of data that allows, persistent identity theft, resulting into denial of the individual's privacy rights; b) Inability to take down content from online publications	1) Unauthorised disclosure of biometrical data (e.g. fingerprint, facial recognition algorithms) which allows recreation of a digital person. 2) Unauthorised access to CRM systems and contract	High	Rare	• Dedicated privacy portal as one-stop-shop • Dedicated mailbox for privacy-related questions which serves as main point of contact for users regarding processing undertaken as part pf TrustPid ecosystem across all parties. Where users contact other parties involved directly, there is an agreed operating model among controllers to collaborate and attend data protection rights irrespective f the channel where the right is exercised. • Ability to manage consents in a self-service portal, or at any involved partner	No

		data bases with signature data. 3) Unauthorised access to security questions.				
Loss of freedom of movement	a) Combination of factors leading to death or bodily harm, embarrassment, abuse, loss of freedom of movement, loss of sense of personal security	1) Risk level would generally be high, unless mitigating factors are present.	Medium	n.a.		
Loss of freedom of association	b) Combination of factors leading to death or bodily harm, embarrassment, abuse, loss of freedom of movement, loss of sense of personal security; b) Denial of membership or access to join or leave a group based on specific attributes of the individual's personal information	1) Risk level would generally be high, unless mitigating factors are present.	Medium	n.a.		
Loss of freedom of expression	a) Combination of factors leading to death or bodily harm, embarrassment, abuse, loss of freedom of movement, loss of sense of personal security	1) Risk level would generally be high, unless mitigating factors are present.	Medium	Rare	• [redacted]	No
Loss of freedom of opinion, religious belief, political opinions	a) Profiling for the purpose of influencing opinions; b) Combination of factors leading to death or bodily harm, embarrassment, abuse, loss of freedom of movement or sense of personal security	1) Unauthorised disclosure of communications content or traffic data 2) Unauthorised access to CRM and analytics systems; 3) Sharing of data to political protagonists and similar	High	Rare	• [redacted]	No

		malicious individuals.				
Bias/Stereotyping / discrimination	a) Disclosure of race, gender, sexual orientation or other sensitive personal data; b) Automated decisions that deem individuals to be dangerous / otherwise undesirable based on a race, gender, sexual orientation or other sensitive data; c) Discrimination based on address, sensitive personal data or other group attributes. Singling out someone for surveillance based on address, sensitive personal data or other group attributes.	1) Risk level would generally be high, unless mitigating factors are present.	High	Rare	• [redacted]	No
Loss of control of purposes of use of personal data	a) Using personal data obtained for a different purpose than was initially declared and outside reasonable expectation of the individual	1) Risk level would generally not be high, unless results in other, more serious harms.	Low	Rare	• [redacted]	No
Loss of opportunity	a) Placing a barrier that limits access to service based on race, gender, health, sexual orientation, religious beliefs or other sensitive personal data, e.g. selecting job candidates by race, gender, health, sexual orientation, religious	1) Risk level would generally be high, unless mitigating factors are present.	High	n.a.		

	beliefs or other sensitive personal data					

3. Suitable measures for identified high residual risks

If there is a high residual risk, other appropriate measures to mitigate the risk must be implemented and tested. The overall result must be documented.

To no.	Countermeasures to mitigate a continued risk (with regard to severity and probability of occurrence)	Controller	Planned implementation date	Implemented on	Checked/ tested by/ on

Result	
☒	No relevant high risks remain after the implementation of suitable measures.
☐	The measures did not eliminate all high residual risks.

4. Consultation obligation

If a process is still exposed to a high risk despite measures taken to mitigate it, the data controller is required in accordance with Art. 36 (1) GDPR to consult the supervisory authority before commencing processing. This process must be documented.
Due to the sensitivities around online targeted advertising considered surveillance we consider it wise to informally consult the regulators in the respective markets where the trial is planned, even if the risk threshold does not meet the criteria for official prior consultation under the GDPR. An informal consultation has been initiated: • Germany – With BfDI; first meeting August 2021 • UK – With ICO, first meeting July 2022 • France – With CNIL, first meeting October 2022 • Spain – With AEPD, first meeting January 2023

5. Acknowledgement and approval

Acknowledgement of the company data protection officer:

DD.MM.YYYY
Date

Mikko Niva (Data Protection Officer of Vodafone Sales & Services Limited)
Signature

Approval by the Business Owner

DD.MM.YYYY
Date

Name (Position)
Signature