04 October 2022

Vodafone Sales & Services Limited
One Kingdom Street
Paddington
London
W2 6BY

RE: VSSL Response to BfDI remarks on the TrustPid service being trialed in Germany received on 25 July 2022

Dear Federal Commissioner for Data Protection and Freedom of Information,

Thank you for your further feedback on our test of the TrustPid service in Germany. We have provided further details and clarifications below in response to the queries and remarks you have raised, as they relate to the processing under the responsibility of Vodafone Sales and Services Limited ("VSSL").

1. Supervisory authority

We acknowledge the BfDI views on this matter and can confirm that we have initiated our engagement with the ICO and have presented to them the solution, including a walk-through of the privacy principles, data flows, consent experiences and assurance processes.

2. Transparent information about the collection, use and processing of personal data

The TrustPid solution has been designed based on a delegated consent model to capture user consent for the various processing activities involved in delivering the service by all the participating parties. To ensure the validity of the consent, a specific design and wording was developed which participating brands and publishers are contractually required to implement.

2.1. Contractual assurances

The Brand and Publisher Commercial Agreements include a schedule specifically outlining responsibilities around obtaining valid consent, including on form and text as described in sections 2.2. and 2.3. below.

2.2. Design specifications/form

Brands and publishers are responsible for collecting the consent on their sites on behalf of the entire TrustPid ecosystem to cover VSSL, Mobile Operators and their own processing. Specifically brands and publishers must:

1. Use the consent wording defined by VSSL in consultation with the participating Mobile Operators (as described in section 2.3. below)
2. Present consent for TrustPid to users within a first layer, separate from descriptions of other cookies, via a separate pop-up to the main Consent Management Portal ("CMP") as shown under Annex 1
3. Enable the user to deny consent as easily as granting it, with one click as shown under Annex 2
4. Provide users with the ability to easily revoke their consent for TrustPid at any time as explained under section 4.2. below

2.3. Consent text

To ensure the consent covers the entire processing related to the enablement of the TrustPid service, the consent wording was updated to the following:

The updated text is currently live with Bild.de only, see Annex 2. The reasoning being that we would welcome BfDI view on the updated consent text as illustrated in this site, before we deploy it to other sites, in case any further changes are recommended.

2.5. Transparency in TrustPid Privacy Portal

The information provided in the TrustPid Privacy Portal was amended on 26 July 2022 to increase transparency on a number of fronts including:

1. Updated Portal text – text has been updated to clarify that service operates only on the basis of user's explicit consent, provide further details on options for revoking consent as well as blocking the service. See Annex 3.
2. Two experiences inside "Manage Preferences" - the user experience and information provided has been enhanced to provide two different experiences for users who have given consent to brand/publisher's website before and users who have not given consent to brand/publisher's website before. Those who have never consented see a confirmation message that their TrustPid is inactive as they have not given consent to any website. See Annex 3.
3. Updated Privacy Notice text – updates to clarify purpose of the processing/service, clarify the data controller, clarify the role of the network operator in the processing, clarify the implications of users' granting consent I.e. processing of traffic data and personalised experience, and retention periods.
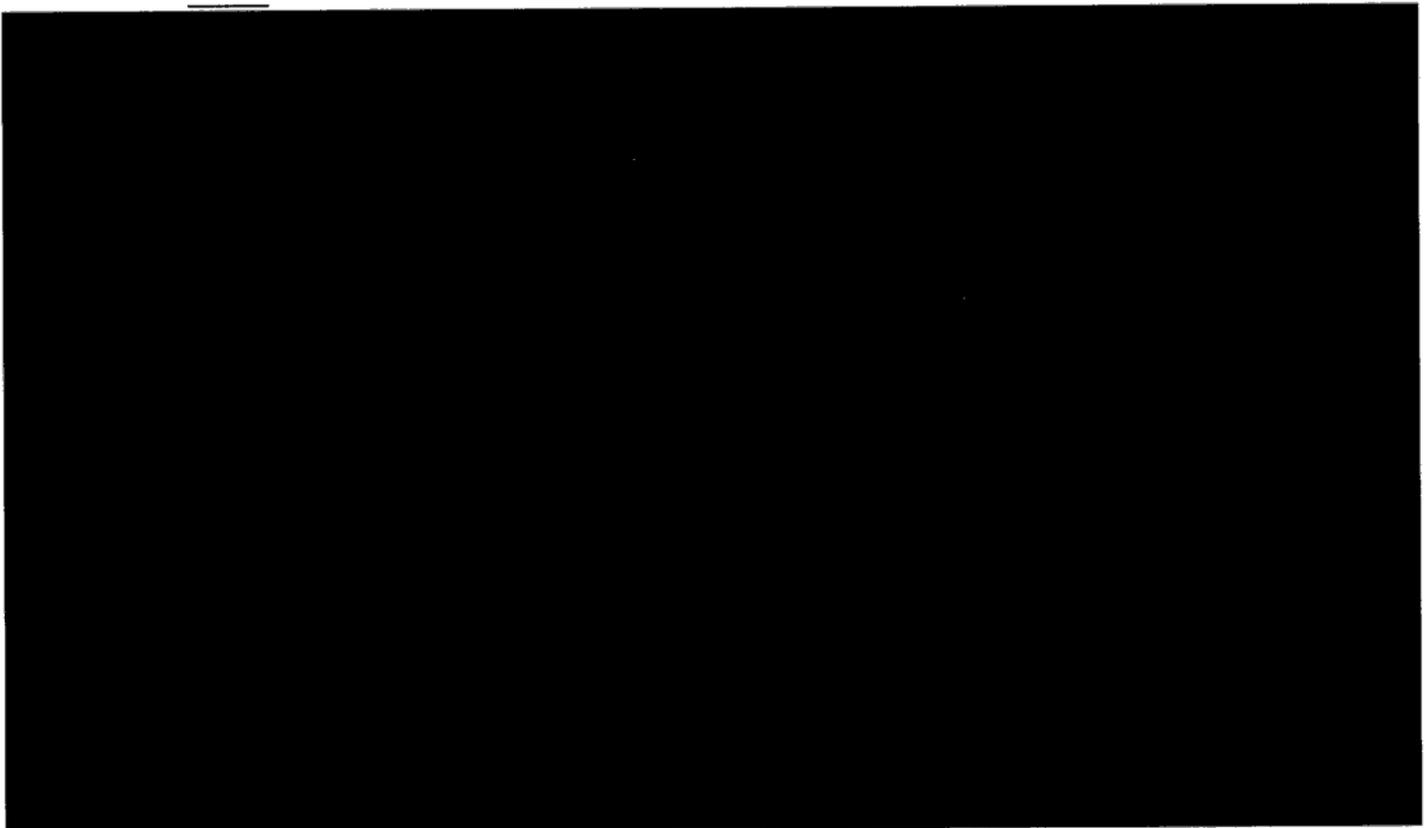
3. Lawful basis for processing

In response to BfDI's remarks regarding the processing and storage by VSSL/TrustPid of the Internet pages visited (with the date of the last update), we can clarify that the lawful basis identified is necessary to provide the value added service which the user has requested by providing their consent as per Article 6(3) of the ePrivacy Directive. The reasoning is that in order to enable the user to effectively manage their consents in one place, we need to store and process the sites visited to reflect where they have consented or not, and record the date of such consent.

We will review the TrustPid Privacy Statement to identify any updates that may be needed to increase transparency of this processing.

With regards to the AdTech ID and MarTech ID stored on the user's device, the lawful basis relied upon is consent under Article 5(3) of the ePrivacy Directive.

4. Possibility of revoking consent, how it is processed in the TrustPid project and communicated to data

Text to be (to be agreed with partners/subject to change):

Consent to the use of TrustPid Service at [INSERT WEBSITE]

Your consent will activate the TrustPid service, provided by Vodafone Sales and Services Limited together with Vodafone and Deutsche Telekom, which allows this website to show you personalized advertising, products and content by digital means.

For this purpose, your IP address will be transmitted to your mobile operator who will identify you and create a pseudonymous network identifier, which is forwarded to TrustPid. [INSERT WEBSITE] will then be provided with marketing token, valid for 90 days. This token along with a related cookie will also be stored on your browser. The token does not directly identify you to the site.

You can find more information in TrustPid's privacy policy [here] and manage or revoke your token permissions via the dedicated Privacy Portal [here] or directly revoke on [INSERT WEBSITE] [here].

Further information about the TrustPid service is also available within the Privacy Policies of the mobile operator Telekom Deutschland GmbH (click here) and Vodafone GmbH (click here).

Previously updated text – currently live:

Consent to the use of TrustPid Service at [INSERT WEBSITE]

Your consent will activate the TrustPid service provided by Vodafone Sales and Services Limited in conjunction with your mobile operator Telekom Deutschland GmbH or Vodafone GmbH. For this service, your IP address will be transmitted to your mobile operator who will identify you and create a pseudonymous network identifier, which is forwarded to TrustPid.

[INSERT WEBSITE] will then be provided with a 90 day marketing token from TrustPid to show you personalised advertising. This token does not directly identify you to the site.

You can find more information in TrustPid's privacy policy.

Further information about the TrustPid service is also available within the Privacy Policies of the mobile operator Telekom Deutschland GmbH (click here) and Vodafone GmbH (click here).

Original text:

Network-based Marketing

["This website" or "Insert P/B name"] can provide you with personalised online marketing based on a unique network token. For this purpose, your IP address is transmitted to your network provider. Based on this, Trustpid creates and manages the marketing token in a way that does not directly identify you to this website. You can find more information in TrustPid's privacy policy here [hyperlink to privacy policy] and manage or revoke your token permissions via the dedicated Privacy Portal here [hyperlink to privacy portal].

The updated text aims to ensure valid consent is obtained for TrustPid by:

1. Specifying the effect of granting consent i.e., activates the TrustPid service to show personalised advertising
2. Identifying all parties involved and how they are involved, namely VSSL as key provider and recipient of the pseudonymous network identifier, Mobile Operators, and the Website (either Brand or Publisher) relying on the consent to conduct their respective processing activities as part of delivering the TrustPid service.
3. Specifying the personal data involved, and particularly highlighting the use of IP address and the creation of the TrustPid identifiers.
4. Clarifying the ways in which user can manage and/or revoke their consent

2.4. Current implementation

All partners currently live in Germany have implemented a separate pop-up dedicated to TrustPid, with the exception of one brand (pilot.de) which has included TrustPid consent in their main CMP whilst still separating it from other cookies (this is a low web traffic partner). See Annex 2 for examples.

By selecting the hyperlink at the footer of the main website which directs the user to a page where they can click a button to revoke TrustPid consent (this does not re-open the TrustPid consent pop-up, but instead directly revokes TrustPid consent upon the button being clicked). We will be reviewing the implementation of the consent revocation journey with Bild.de to explore any further improvements that can be made to the journey.

All other live websites:

By accessing the website's privacy policy which includes reference to TrustPid service and selecting the hyperlink to re-access the TrustPid pop-up in their site to amend their preferences. We are working with our partners to explore what improvements can be made.

How long does it take to come into effect?

Effect is immediate. The change to consent status and cease of processing happens in real time.

How is this synchronised to the Portal?

4.2. Options for revoking consent/objecting to the TrustPid processing

There are two ways to stop the TrustPid service:

4.2.1. Revoking consent:

A) On Publisher/Brand website

How can the user do this?

Currently, there are two models on how user can re-access the consent pop-up for TrustPid to remove their consent.

Bild.de:

Manage your Preferences

By tapping on the 'Manage Preferences' button, you can review and manage your settings and preferences for the TrustPid service

When you click on the 'Manage Preferences' button, we will process your data as described in the Privacy Notice to contact your mobile operator to provide you access to the TrustPid Privacy Portal

Manage Preferences

Please note that you must use a mobile internet connection. If you have Wi-Fi enabled, turn it off and click Refresh.
You might not be able to access this section with an active AdBlocker.
If your mobile operator does not participate in the TrustPid trial operation, a TrustPid token will never be created for you. In this case, you will also not be able to manage your settings and preferences through the Privacy Portal.

Please visit our Privacy Notice for more information.

Your TrustPid service is active

The list below lists all websites to which you have given consent for the use of a TrustPid token in the past.
You can manage your preferences for the TrustPid service individually for each website by clicking on the relative button in the list below. You can also manage your preferences for the TrustPid service as a bundled form.
Alternatively, you can also block the service and prevent the re-activation.

Further information can be found in our Privacy Notice.

Block Service and prevent re-activation

This option prevents the use of the TrustPid service. You will then no longer participate in the TrustPid service (even if you have given your consent before or after). TrustPid tokens will then no longer be created or shared (even if consent is given afterwards). Unless you unblock the service and give new consents on participating websites. You can unblock the service at any time via the TrustPid Privacy Portal.

Block service ✕

Remove all

You can block websites from using your TrustPid token that you have previously given consent to on their websites with one click. However, you can still be asked for consent on corresponding websites and thereby share a TrustPid token. If you want to prevent anyone from using your TrustPid token even when you are asked for consent, use the function "Block service"

Remove all ✕

✕

We have made adjustments so that it is also possible for user to enable the block service feature without having given any prior consent. In this case once the user lands on the Manage Preferences site of the Privacy Portal they would be presented with a notice that their service is inactive and offered the option to "Prevent activation".

Your TrustPid service is inactive.

You have not given consent to any website.
If in the future, you do provide consent to one or more websites then you will be able to view and manage your preferences for the TrustPid service on this portal.

The TrustPid service can only be activated with your consent and agreement.

If you want to prevent the activation of the service, even if you give consent in participating websites afterwards - you can do so by clicking on the button "Prevent activation" below

✕

Your TrustPid service is inactive.

You have blocked the service.

In order to use the TrustPid service, you must first unblock the service. To do this, please click on the button "Unblock service"
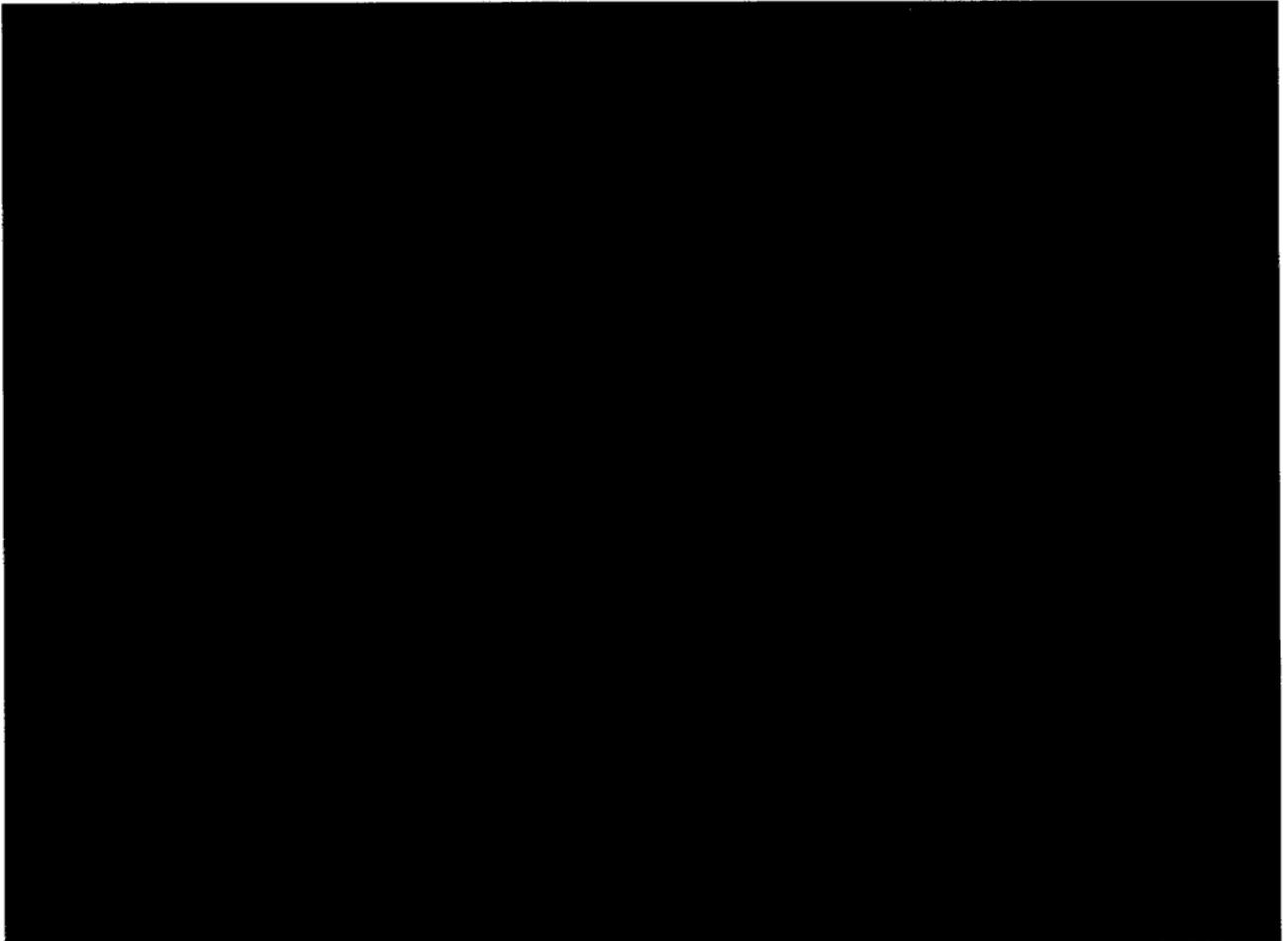
Unblock Service

How long does it take to come into effect?

There are no issues with synchronisation where a user revokes consent on the Brand or Publisher's website which is then reflected in the TrustPid portal as explained above.

B) On TrustPid Privacy Portal

How can the user do this?

The user needs to access the TrustPid Privacy Portal and navigate to Manage Preferences area where they will be required to verify themselves, by clicking the "Manage Preferences" button, to ensure only the user can change their own preferences. Once inside, the user is able to revoke consent for one specific website or in bulk.

4.2.2. Object to the processing via "Block service" on TrustPid Privacy Portal

How can the user do this?

The user needs to access the TrustPid Privacy Portal and navigate to Manage Preferences area where they will be required to verify themselves to ensure only the user can change their own preferences. Once inside, the user is able to select the "Block Service" button.

Participating Mobile Operators have included the following wording in their websites:

"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"

B) Publisher/Advertiser websites:

Currently all live websites make reference to TrustPid in their own privacy statements 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 or to re-access the TrustPid pop-up in their site to amend their preferences.

In response to the BfDI's remark on the implementation of the revocation options of our partner, n-tv.de, specifically, that there is no reference to TrustPid in the "Privacy Center" of this website, we have revisited the experience and have engaged with our partners to increase transparency and accessibility for user of revocation options. Specifically, we have initiated discussions with RTL to explore the implementation of the BILD.de approach of inserting a hyperlink at the footer of the site to enable consent revocation to TrustPid.

TrustPid consent revocation is not referenced in the "Privacy Centre" of the website as we have taken the same design approach as with the granting of the consent. Namely, to keep Trustpid clearly separate from other cookie processes. In this context, as the "Privacy Centre" in this website is specific for the management of the site's cookies, we did not incorporate consent revocation for Trustpid in this area which is dedicated to cookies.

5. Consent Assurances

5.2. Ensuring correct implementation on partner sites

We monitor live Advertisers and Publishers on a weekly basis to ensure that an agreed and compliant consent experience is put in place by the Advertisers and Publishers and to stop sending to Telco requests for the provision of IDs as soon as noncompliance is detected by such monitoring or is notified by Telco to Vodafone.

The checkpoints screened during the weekly routine are:

- Screenshot of the TrustPid consent banner for track record
- Use of the coordinated consent text
- Separation of TrustPid purpose from other purposes in the cookie banner
- Rejection possible in one click
- Buttons for approval and rejection on an equal footing
- Linking the TrustPid Privacy Notice
- Linking the TrustPid Privacy Portal
- Possibility to revoke the TrustPid consent on the partner site
- Possibility to call up the Privacy Portal again at any time

Duration of the block - We have now made fixes to ensure that an objection to Vodafone Sales and Services Limited (at www.trustpid.com) is not limited to 90 days. Instead, adjustments have now been made to ensure the block remains in place indefinitely.

How long does it take for the block to apply once user activates it? The block is implemented in real time on the TrustPid platform.

How is this synchronised against the websites?

Block Service has the effect of deleting all website "consents" i.e. all ID graph entries are deleted in the TrustPid platform. On the website, the user may still appear as consented for a maximum of 10 minutes after activation of the block due to the 10 minute check on client side.

In scenarios above where use of IP address is in scope, this is flagged to the user in the just in time notice provided before the user clicks to access the Manage Preferences area of the Privacy Portal. We will review the text presented to identify any updates that may be needed to further increase transparency.

4.2.3. Revoking consent directly from the Mobile Network Operator

Currently we do not enable consent revocation/blocking the service directly from the telecommunications provider sites e.g. via a telco self-service portal as we have designed our solution to provide a self-serve one-stop-shop portal to enable users to manage their preferences without having to do it individually visiting each site. This feature provides a better user experience by avoiding fragmentation and variation in information provided and keeping management of permissions in once place, facilitating understanding and control to individuals. Enabling consent revocation/blocking the service directly from the telecommunications provider sites would require reliance on an end user's account; our service relies on a connection rather than an account therefore it would require an understanding of how to best implement this whilst maintaining the principle of offering a service decoupled from operators. Additionally, we considered that such implementation could impact the user experience and possibly clarity around whether or not TrustPid service is enabled or not, since in order to synchronize the block on a telco side with our server so as not to continue showing consent pop-up to the user that blocked on the telco side, would possibly require additional data processing. However, we will seek to explore options with our Telco partners in this respect.

4.3. How the options to revoke consent/block service are communicated to users:

4.3.1. At first point of contact via consent text

The consent text has been updated to bring further transparency to users on options to revoke consent. Specifically, the updated text indicates:

> "You can find more information in TrustPid's privacy policy [here] and manage or revoke your token permissions via the dedicated Privacy Portal [here] or directly revoke on [INSERT WEBSITE] [here].
>
> Further information about the TrustPid service is also available within the Privacy Policies of the mobile operator Telekom Deutschland GmbH (click here) and Vodafone GmbH (click here)."

4.3.2. Via the Privacy Portal

Within the Privacy Notice section of the Portal, we inform users:

> "**Consent you provide** to advertisers and publishers on their websites. You can withdraw this consent for the TrustPid service at any time via the Cookie Management Platform of advertisers and publishers or via the TrustPid Privacy Portal."

4.3.3. Via the participating partner websites

A) Mobile Operators websites:

The contract templates for VSSL and brand/publisher were also updated to clarify and strengthen responsibilities for brands and publishers around obtaining consent and thus provide further assurance to Mobile Operators.
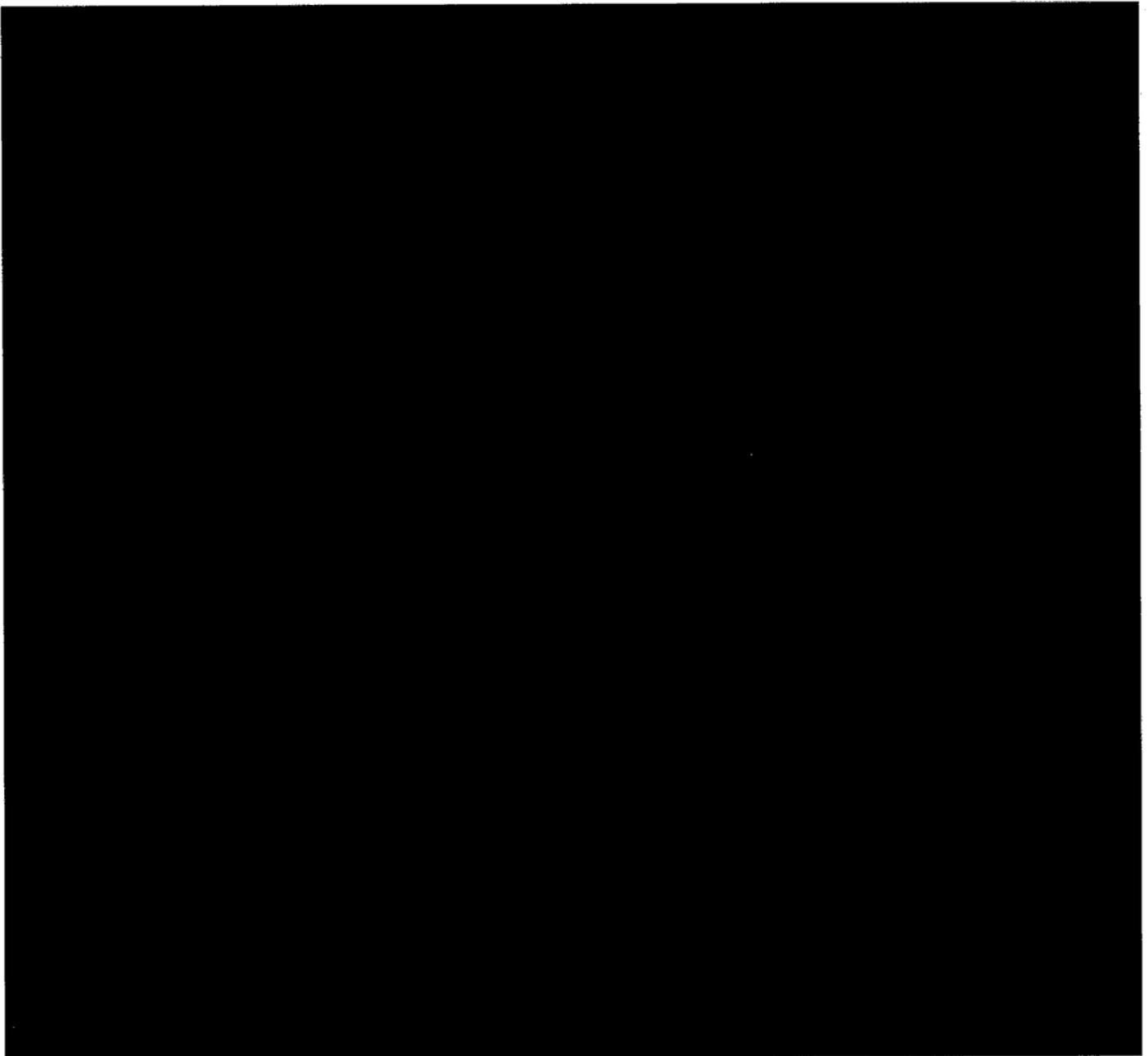
As it stands one partner is operating under Joint Controllership basis for the MVP. The updated contracts will be used to inform the development of the Joint Venture, and seek to reflect Joint Controllership only amongst partners involved in the Joint Venture.

7.2. VSSL and Mobile Operators

As it stands, contracts between VSSL and Mobile Operators have been concluded on an Independent Controller basis, however, this position would be changed to Joint Controllership as part of the Joint Venture development.

8. Data Protection Impact Assessment (DPIA)

Further to the BfDI remarks regarding the DPIA, we are taking steps to amend the same in line with feedback received.

6. Data privacy compliance in the case of shared use of a mobile connection

There are two scenarios where users can share a connection:

1) Using a mobile Wi-Fi hotspot (mobile broadband device):

Currently users relying on mobile Wi-Fi hotspot, meaning a device with a sim that connects to the network (e.g. dongle) ,are ineligible for the service. Users browsing with mobile Wi-Fi hotspot are excluded from the solution, meaning that no identification would take place for these users and service would not be enabled. Eligibility of users relying on mobile Wi-Fi hotspot is being explored, where such usage would fall into the "fixed" user access scenario and would be based on the concept of household.

2) Tethering:

Users relying on data connection shared by other users (Tethering) are eligible to use the service. In such cases, users would have access to the same portal and visibility of the websites visited by anyone browsing on the shared connection.

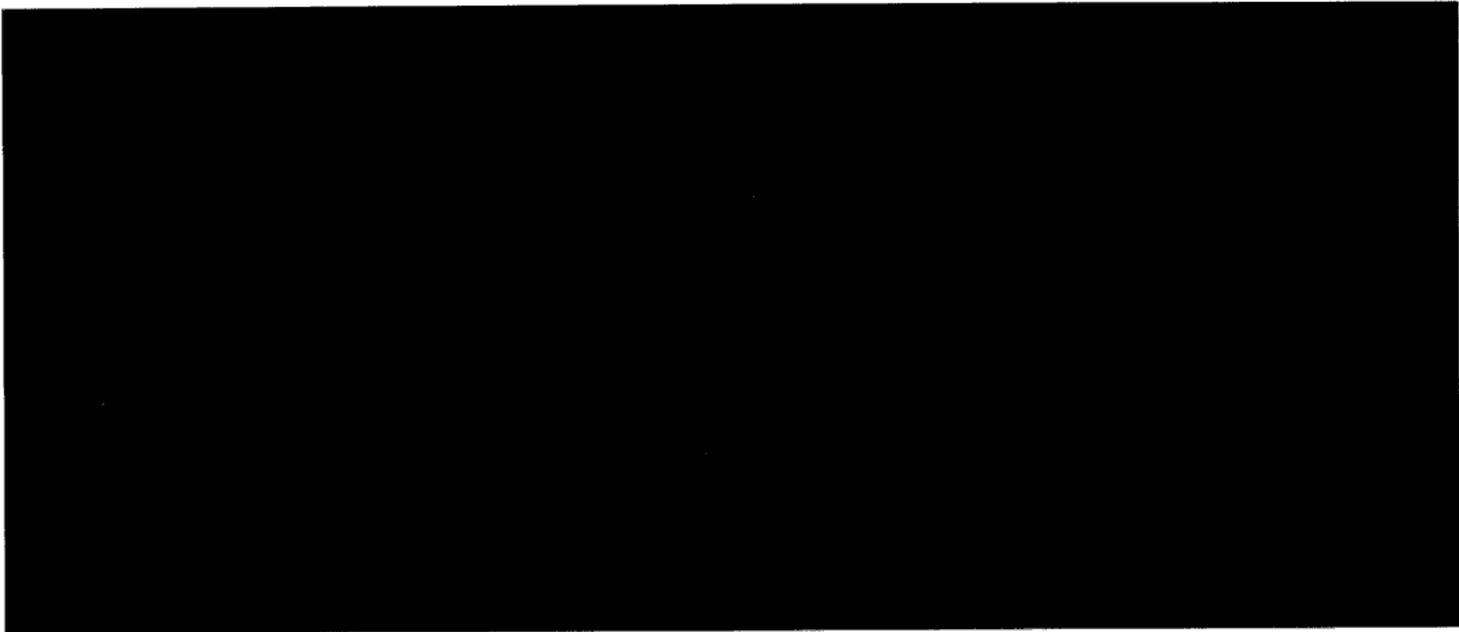Our Privacy Portal currently informs users of the following:

> "If you have enabled a hotspot or tethering connection, please note that anyone using the same hotspot or tethering connection can see and manage the same information in the Privacy Portal. This is due to the technical conditions in the context of the current test operation of TrustPid."
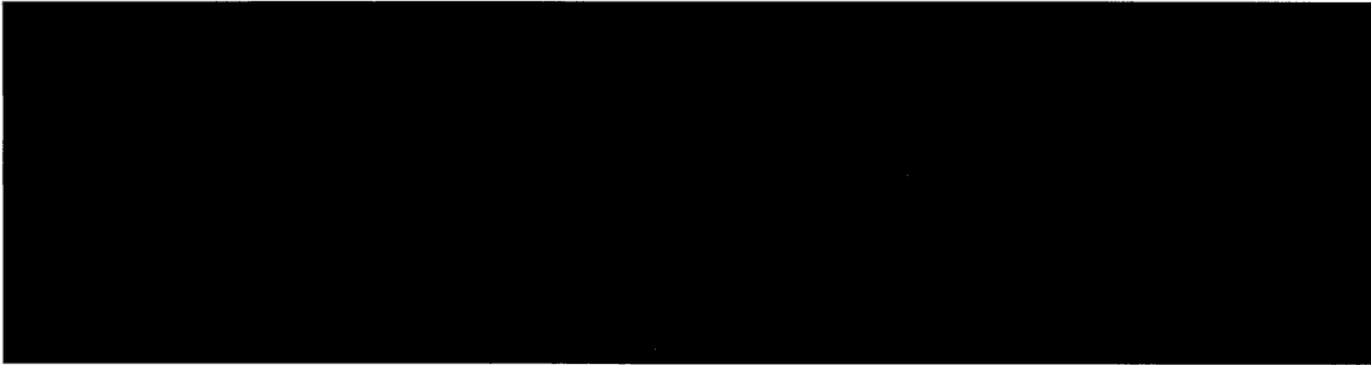

7. Responsibility under data protection law and contractual agreements

7.1. VSSL and Brands/Publishers

Contract templates between VSSL and website operators have been updated to reflect Joint Controllership. Specifically Joint Controllership has been defined for the identification and generation of unique IDs (UMID, AdTech ID, and MarTech ID) based on hashed MSISDNs to implement the Services, as well as for the provision of AdTech ID and MarTech ID through browser or app data layer, enabling advertising solution based on a stable telecommunications network identity.

We hope the additional information provided addresses your queries.

Yours faithfully,

Vodafone Sales and Services Ltd.
Vodafone House, The Connection Newbury, Berkshire RG14 2FN

6844137

Einwilligung in die Nutzung von TrustPid bei sport.de

Diese Webseite kann Ihnen personalisierte Werbung und Inhalte auf der Basis einer netzwerkbasierten Marketing-Kennung anzeigen. Dafür wird Ihre IP-Adresse an Ihren Netzbetreiber übermittelt. Auf dieser Grundlage erstellt und verwaltet „TrustPid" Ihre Netzwerkkennung, über die Sie für die Webseite für einen begrenzten Zeitraum wiedererkennbar sind, allerdings nicht als Person. Mehr Informationen finden Sie in den TrustPid Datenschutzhinweisen. Ihre Einwilligungen können Sie jederzeit auch über das Datenschutzportal widerrufen und managen.

Akzeptieren

Ablehnen

Sofern Sie akzeptieren, wird die TrustPid im Rahmen der von Ihnen im vorhergehenden Einwilligungsdialog bereits erteilten Einwilligungen für die dortigen Zwecke und Vendoren genutzt. Einstellungen hierzu können Sie im Privacy Center treffen.

Datenschutzerklärung | Impressum

Annex 2 – Current TrustPid Consent Implementation

Bild.de:

RTL:

What is TrustPid?

Consumers appreciate 'free' content and services on the internet. In order to be able to provide high-quality content, publishers, internet services and apps rely on advertisers who display targeted advertising.

The amount and type of information that advertising technologies generate about consumer interests raised privacy concerns.

Tokens for continued free internet content

TrustPid is a technology solution that allows consumers to enjoy free content and the benefits of the open internet whilst maintaining control over their privacy.

TrustPid works with secure, unique digital tokens generated by assigning random numbers. It is not possible with the tokens to directly identify you as a person. Nevertheless, a token allows advertisers and publishers to provide you with a personalized experience on their websites, apps and services, if you have given your explicit consent.

Detailed and transparent information about how we generate and manage your TrustPid tokens can be found in the Privacy Notice.

Your consent to TrustPid is obtained from advertisers and publishers when you access or use their websites, apps or services. Your consent is voluntary and only applies to the respective websites.

Full control in the Privacy Portal

TrustPid gives you complete control over how your tokens are used. You can manage your preferences for the TrustPid service at any time via the central dashboard in TrustPid's Privacy Portal. In the Privacy Portal you can see which advertisers or publishers you have allowed to provide you with personalised online marketing on their websites.

You can also block TrustPid completely if you want to prevent tokens from being given to advertisers or publishers even though you have given consent.

Annex 3 – TrustPid Privacy Portal

TrustPid

What is TrustPid?

With TrustPid, you retain full control over your digital data while browsing the internet and using your smartphone apps. TrustPid is a cross-operator test platform for data protection-compliant digital marketing. The focus of the test is to check the technical feasibility.
You can use TrustPid voluntarily if you are a customer of one of the participating network operators and visit a supported website or app and give your consent there.

READ MORE

What is TrustPid Privacy Portal?

Through TrustPid Privacy Portal, you have full control over your TrustPid configuration as well as the websites and apps you have consented to use TrustPid tokens. Among other things, you can manage your preferences or block the service entirely.

READ MORE

Find out more about TrustPid

READ MORE

Manage your Preferences

By tapping on the 'Manage Preferences' button, you can review and manage your settings and preferences for the TrustPid service.

When you click on the 'Manage Preferences' button, we will process your data as described in the Privacy Notice to connect your mobile operator to provide you access to the TrustPid Privacy Portal

Manage Preferences

Please note that you must use a mobile internet connection. If you have Wi-Fi enabled, turn it off and click 'Refresh'. You might not be able to access this section with an active AdBlocker
If your mobile operator does not participate in the TrustPid trial operation, a TrustPid token will never be created for you. In this case, you will also not be able to manage your settings and preferences through the Privacy Portal

Please visit our Privacy Notice for more information.

About Us

We are Vodafone Sales and Services Limited. Our registered office is Vodafone House, The Connection Newbury, Berkshire RG14 2FN. We are registered in England under company number 06844137

We are testing a new technology solution called TrustPid. TrustPid is a technical solution for digital advertising in Europe. Since it is a consent-based solution and you can adjust your settings and preferences at any time via the Privacy Portal, the solution offers you full, privacy-compliant control over your settings and preferences.

In the TrustPid process, the telecommunications providers provide the network-based infrastructure for the service. If you actively agree as a customer, you create a pseudonym by processing your IP address. On this basis, further pseudonymous tokens are created, which are then managed by TrustPid. In addition, the network operators or TrustPid do not pass on any customer data, such as demographic or network data.

For more information or questions, please visit our Privacy Notice or contact us by sending an email to advisor@trustpid.com

PRIVACY NOTICE

Find out more about TrustPid

Advertising on the Internet is currently in the hands of few dominant platform operators.

This dominance could increase further with the imminent end of so-called third-party cookies - which are problematic from a data protection point of view.

Publishers that urgently depend on advertising to support the creation of content, are therefore looking for ways to become more independent, whilst at the same time maintaining European protection standards so that customers retain complete ownership of their data through transparency and control.

Vodafone Group is currently conducting a test involving other European telecommunication providers including Deutsche Telekom and a few advertisers and publishers to investigate the benefits of a new technical solution to facilitate digital advertising and marketing.

We are in ongoing discussions with the Federal Commissioner for Data Protection and Freedom of Information (BfDI) about the solution being trialed.

The focus of the test is to examine the technical feasibility.

Consumers, advertisers, and publishers could all benefit from this technology in the future.

TrustPid is the name of this test platform, which is available to interested customers of the participating telecommunications providers.

These customers can try out the new approach for the duration of the test - participation is only possible after having previously given voluntary and explicit consent (so-called opt-in).

TrustPid is a cross-operator infrastructure for digital advertising and digital marketing.

It is to be seen as an alternative to the dominant platforms and a counter-design to the third-party cookies still present today.

In the TrustPid process, the telecommunications providers provide the network-based infrastructure for the service. They create pseudo-anonymous tokens for the customer - provided the customer actively agrees - by processing the customer's IP address. This serves as the basis for creating tokens, which are then managed by TrustPid.

For a single user, the token generated will be different for each different partner. This limits the merging of data from different partners to create profiles on customers - one of the big drawbacks for consumers in the way digital advertising works today.

The telecommunications providers do not observe the website which any customer or which internet is the provided by the service in any other way.

Neither the partners, nor TrustPid itself, can identify an individual by means of the token created by TrustPid.

The solution aims to enable personalized product recommendations on the Internet that many users want, but in a secure and privacy-friendly way.

In this way, we want the availability and diversity of content in the future as well.

There details for the customer to activate this service.

They can revoke their given consent centrally at any time and block the service.

This declaration will not be automatically reactivated under any circumstances.

They can trust that their data will be handled with care and used only for purposes to which they have explicitly consented. Of course, all parties involved in this test comply with the requirements of the General Data Protection Regulation (GDPR), as well as all other applicable laws.

The TrustPid trial currently being undertaken in Germany does not automatically mean that the technology will be formally launched as a commercial proposition.

What is TrustPid Privacy Portal?

The Privacy Portal is a central, user-friendly self-service area that shows you all consents already given. Here you have the option of revoking the consents you have given individually or bundled for the TrustPid service. In addition, you can block TrustPid service in the Privacy Portal. In this case, any consent you have given on individual websites will be prevented by TrustPid – so you will not participate in the TrustPid service even if you give your consent. Unless you unblock the service again.

In the Privacy Portal, you can do the following at any time:

- Check the list of advertisers and publishers with whom you have given consent, i.e. to whom you have allowed the use of a TrustPid token. You will also see when this consent has been obtained and until when it is valid.
- Manage your preferences for one or more websites for the TrustPid service.
- Block the service: The TrustPid service is then completely suspended. This means that TrustPid tokens will then no longer be created or passed on to websites (even if consent is given afterwards) (for more information on our data retention period, please see our Privacy Notice).
- Find contact details: If you need more information or wish to exercise your data protection rights in accordance with the Privacy Notice.

Please note, exercising your preferences via the TrustPid portal is limited to tokens stored on the TrustPid platform. Participating websites may still use cookies or other tracking technologies to provide you with a personalised browsing experience. To manage these, please visit the website's specific cookie policy. In order to delete these please ensure to clear your cookies via the browser.

Special features of blocking the service and the use of hotspots/tethering

Please note that in the short term it may still look as if the service is active, even after you have blocked the service. However, rest assured that your TrustPid token will no longer be used. If you have previously actively participated in the TrustPid service, any related advertising will be stopped within a maximum of 24 hours of your blocking of the service

If you have enabled a hotspot or tethering connection, please note that anyone using the same hotspot or tethering connection can see and manage the same information in the Privacy Portal. This is due to the technical conditions in the context of the current test operation of TrustPid.

Two experiences for "Manage Preferences":

Manage your Preferences

By tapping on the 'Manage Preferences' button, you can review and manage your settings and preferences for the TrustPid service.

When you click on the 'Manage Preferences' button, we will process your data as described in the Privacy Notice to contact your mobile operator to provide you access to the TrustPid Privacy Portal.

Manage Preferences

Please note that you must use a mobile internet connection. If you have Wi-Fi enabled, turn it off and click 'Refresh'.
You might not be able to access this section with an active AdBlocker.
If your mobile operator does not participate in the TrustPid trial operation, a TrustPid token will never be created for you. In this case, you will also not be able to manage your settings and preferences through the Privacy Portal.

Please visit our Privacy Notice for more information.

Your TrustPid service is inactive.

You have not given consent to any website.
If in the future, you do provide consent to one or more websites then you will be able to view and manage your preferences for the TrustPid service in this portal.

The TrustPid service can only be activated with your consent and agreement.

If you want to prevent the activation of the service, even if you give consent in participating websites afterwards - you can do so by clicking on the button "Prevent activation" below.

Prevent activation ✕