



# Data protection information of Telekom Deutschland GmbH ("Telekom") for the website

## General

The protection of your personal data is a high priority for Telekom Deutschland GmbH. It is important to us to inform you about what personal data is collected, how it is used and what options you have in doing so.

## What data is collected, how is it used and how long is it stored?

- a) Necessary processing in the provision of the digital service (Art. 6 para. 1b GDPR, §25 para. 2 no. 2 TDDDG)

When **using the website**, referred to in the following digital service: You can find out about products and services of Telekom Deutschland GmbH. If you place an order in the digital service, we will record the contact, payment, and order data you have entered for the purpose of processing the request and store it until the end of the contract period, but other statutory retention periods may apply beyond that.

- For the **legitimacy check** in the context of concluding a contract, we use the "Video Ident" service of the processor [Purpleview GmbH](#) (Kampstraße 6, 44137 Dortmund) within the video chat. In addition, we also offer video consultation as a contact channel for all customers. If you use this offer to contact customer service, technical data and, if applicable, contract data in the case of Video-Ident will be transferred to the customer advisor when the chat is initialized. Communication data that is exchanged within the conversation via video or chat is not stored, including the name provided. When making an appointment, your name, e-mail address and optionally the phone number will be deleted over the period of use plus 7 days after the appointment. Cookies are set for the duration of the session, which are deleted at the end of the session or after 12 hours at the latest. Data that you provide to us in the chat will be processed exclusively for the purpose of processing your request. The deletion takes place after the end of the call. For translation into other languages, Deutsche Telekom uses the service of Chatlingual, 1801 Wewatta Street, Floor 11, CO 80202, Denver, USA. The data is deleted there immediately after processing. For error identification and troubleshooting, we only store the activities and events about the session, in particular the beginning and end of the session and browser version for 14 days. In the event of improper and abusive use of the video chat (e.g. through obscene gestures, repeated insults, etc.), the Consultant has the option of terminating the chat and storing the following data of the User: consent to the Terms of Use, IP address, session ID of the chat, the transmitted image (only when the camera is activated on the User's side). The storage option is only used in individual cases to protect chat employees and serves both to deter misuse and to identify the user to be able to initiate clarification and, after examination, possible further measures. The data is stored for a maximum of 30 days. We reserve the right to carry out the statistical evaluation of anonymised data sets.

- b) Additional processing in the provision of the digital service that is carried out on the basis of consent, e.g. optionally offered communication channels (Art. 6 para. 1a GDPR, §25 para. 1 TDDDG)

**User Surveys / Customer Feedback:** We use the "Get Feedback" service provided by [SurveyMonkey Europe UC](#) (2 Shelbourne Buildings, 2nd Floor, Shelbourne Road, Ballsbridge, Dublin 4, Ireland) (Note: SurveyMonkey has acquired the previously used company Usabilla and its tool of the same name). Ratings and your feedback can be requested. Our customers' opinions and suggestions for improvement are important components for the improvement of our digital services. Only the data that you provide to us will be processed (Art. 6 para. 1a GDPR). The data will be stored and evaluated by us for 24 months. The surveys can be carried out in two different ways:

- i. The feedback button. You can use this button to give us your feedback at any time. If you do not use this function, no data will be transmitted.
- ii. Overlay of an active feedback query. You can deny this query or cancel it at any time. The answers will not be

sent until you complete the survey.

**Chatbot:** If you use the "Ask Magenta" chatbot as a self-service or for contact with customer service, various information is transmitted to the dialogue platform during the automated chat. This includes, for example, the questions and answers you enter (chat history) or your customer data if you have logged in in advance with the Telekom login.

To give you a more appropriate answer to your questions, we use artificial intelligence (AI). If you send your request to this service via text message, we replace your personal data such as name, address, telephone number or email address with placeholders before we have it processed by the actual AI system (so-called pseudonymization). The AI is then trained later with anonymized chat histories. The privacy notice for Textchat [applies to the use of this service](#).

**Text Chat:** If you use Text Chat to contact customer service, various information will be transmitted to the customer service representative when the chat is initialized. This includes login data, customer data (phone number, customer number and current chat history), as well as the help topic you have selected, browser version, operating system version and the like. To identify errors and troubleshoot technical complications, communication metadata (such as timestamp, session ID, forwarding) and supplementary information (such as device used, operating system, etc.) are stored. The communication metadata and message content of all chats, including personal data, will be stored for up to 8 days if you are not a Telekom customer. In addition, the chats are anonymized. If there is a contractual basis, i.e. you are a Telekom customer, we usually store the logs and communication metadata in accordance with Section 257 of the German Commercial Code (HGB) as commercial letters, as well as the anonymized chats and pseudonymized metadata for customer support in follow-up contacts and for quality improvement. In addition, information about the accessibility of the chat service is transmitted at regular intervals from the chat platform of our processor [Genesys Telecommunications Lab. GmbH](#) (Herzogspitalstraße 24, 80331 Munich). For this purpose, a session cookie is set for the duration of the session, which is deleted at the end of the session. We reserve the right to carry out the statistical evaluation of anonymised data sets.

**SMS messaging:** When you use SMS messaging to contact customer service, various pieces of information are collected during the first contact. This includes, for example, the mobile phone number, first and last name and which issue is affected. The processing takes place via the internal chat platform of Deutsche Telekom, as well as the processor [Genesys Telecommunications Lab. GmbH](#) (Herzogspitalstraße 24, 80331 Munich). We store the content of the session for a maximum of 12 months in order to be able to access it in case of queries. We reserve the right to carry out the statistical evaluation of anonymised data sets.

**Telekom helps community:** Deutsche Telekom operates the Telekom helps community for the purpose of supporting people who have questions and/or feedback about products and services from the Telekom portfolio and/or would like to exchange ideas with other people about these topics. You have the option of having your personal data deleted from the Telekom hiltf Community at any time. Your profile will be cleaned of personal data and anonymized. Posts created by you will remain anonymous in the Telekom hiltf Community and will continue to be accessible to all visitors to the Telekom hiltf Community. This is done without naming your username. The Telekom hiltf community is based on a product from [Sprinklr Inc.](#) As a processor, the latter has access exclusively for the purpose of operating and maintaining the platform.

**Stay logged in:** If you log in with your email address or mobile phone number and password, the browser can remember this information. As soon as you check the box, you do not have to log in every time you want to use your Telekom account. Nevertheless, you will be asked to enter your password again if you have not used the [Telekom login](#) for more than 6

months or if special personalized services request this. You can log out of your Telekom account at any time by clicking on the "Unsubscribe" link in the navigation bar. Once you are logged out, you can log in again and check or uncheck the box again.

**Remember username:** Your browser can remember your username when you log in with Telekom Login if you check the box. This means that you don't have to enter your username again the next time you log in. If you have not used the Telekom Login for more than 180 days, you will still be asked to enter your username again. You can log in to Telekom Login at any time with a different username.

**Connection of Telekom routers:** The Customer Center enables the configuration of Telekom routers (e.g. Speedport Smart 4, Speedport Pro). The router is automatically detected based on the Telekom Login without having to re-enter the access data or the device password. The customer center provides a protected interface for this purpose, which makes it possible, among other things, to change the Wi-Fi password and the Wi-Fi name (SSID) of the router, but not to read existing passwords.

During the **availability check**, your address data is stored as a hash value in a cookie for 14 days.

#### a) Different processing in TelekomCloud Marketplace (business customers)

- 1. Text Chat TelekomCLOUD Marketplace:** If you use the text chat on the TelekomCLOUD service to contact customer service, various information is transmitted to the chat system (Art. 6 para. 1 b, f GDPR) and deleted after 7 days. These include, for example: Your IP address, browser version, operating system version; this data cannot be viewed by our customer advisor. The data generated during the Service Chat is transferred to our CRM system. The chat content is deleted after 24 hours at the latest due to the system. Additional data about the chat (start time, duration of the chat, internal notes, customer information requested in the chat if necessary) will be anonymized after 28 days. In addition, information about the accessibility of the chat service is transmitted from the chat platform to the digital service of the TelekomCLOUD Marketplace at regular intervals. With the help of this information, the button to start the text chat is activated or deactivated on the digital service.

We use your personal data only for the purpose of technical administration of the digital service and to fulfil your wishes and requirements. Additional personal data, such as Your name, address, telephone number or e-mail address will not be collected, unless this information is provided by you voluntarily (Art. 6 para. 1a GDPR) or in connection with registration on the TelekomCLOUD Marketplace (Art. 6 para. 1b GDPR). The data you enter when contacting us, the scope of which can be found in the contact form, will be processed exclusively for the purpose of structuring the response to inquiries and the provision of services by Telekom Deutschland GmbH. Only if you have given us your consent in advance, we will also use this data for product-related surveys and marketing purposes – but only to the extent necessary for each specific case and in accordance with the consent given (Art. 6 para. 1 a GDPR). Personal data will only be passed on to third parties with the express consent of the person concerned. Our contractual partners are contractually obliged by us to treat your data confidentially and in accordance with the legal regulations. You can decide for yourself whether we may use your data for our own marketing purposes when you register. You will only receive advertising information from us if you consent to such use. You have the option at any time to object to such use and to revoke any consent you may have given for the future. If you register, we process and use the contract data collected at the conclusion of the contract and during the term of the contract, which is necessary for the reciprocal and proper performance of the contract, as well as the voluntary information (contract data). Contract data includes title, surname and first name, address, date of birth, telephone number and/or e-mail addresses, data on payment processing and sales data – differentiated according to the services, products used and information about the products you use. If you set up additional users, their data will also be stored. Your contract data will only be stored beyond the end of the contractual relationship in accordance with the contractual agreements and will be limited to the minimum necessary in each case. We store the text of the contract and send you the order data by e-mail. Your contract data will be deleted no later than 90 days after the termination of the contractual relationship by deleting your user account. Usage and billing data: We store and use billing data for the proper provision of our services and for billing purposes. Billing data includes information about the start and end of each use and the services used.

#### Processing customer data with Salesforce:

To process customer service inquiries and to communicate with customers by e-mail or telephone in accordance with your consent, your personal customer data will be stored and processed in our CRM system. We use the

services [Salesforce Service Cloud & Salesforce Marketing Cloud](#) of the processor [Salesforce \(Salesforce.com Germany GmbH, Erika-Mann-Str. 31-37, 80636 Munich, Germany\)](#).

If you have given us your consent, we will collect email usage information (sending, openings, clicks) via this system to improve our service to you and to provide you with more relevant information. If you no longer agree to this, you can object to this at any time under "My settings".

**Customer feedback with Salesforce Survey:** If you use our support services, we may invite you to participate in a customer satisfaction survey via email. Participation in the survey is voluntary and serves to improve the quality of our services. In this case, the results of the survey are linked to the corresponding customer case and stored in a personalized manner to be able to evaluate the associated service in a targeted manner. To complete the survey, you will be redirected to the website of Salesforce (Salesforce.com Germany GmbH, Erika-Mann-Str. 31-37, 80636 Munich, Germany). You can find more information about their legal and data processing principles under <https://www.salesforce.com/company/legal/>.

- Processing in the provision of the digital service that is carried out based on legitimate interest (Art. 6 para. 1 f GDPR, §25 para. 2 no. 2 TDDDG)

- When you use our digital service, our servers temporarily record the domain name or IP address of your device as well as other data, such as the requested content or the response code. The logged data is used exclusively for data security purposes, to defend against attack attempts on our server. They are not used to create individual user profiles or passed on to third parties and are deleted after 7 days at the latest. We reserve the right to carry out the statistical evaluation of anonymized data sets.

**Fraud prevention:** To avoid cases of fraud in our online service, we have commissioned the company [Risk.Ident GmbH](#) (Am Sandtorkai 50, 20457 Hamburg) to provide the service. Risk.Ident collects and processes data on the pages of our online shop with the help of cookies and tracking technologies to determine the end device used by the user. If IP addresses are collected by Risk.Ident, they are immediately anonymized. The data processed by Risk.Ident is stored in a database for fraud prevention. We access these as part of the ordering process for the purpose of a risk assessment. In addition, we transmit data to Risk.Ident on end devices from which (attempted) fraud has already occurred. The data is not assigned to persons at any time.

**Other:** Here you will find further information on the topic [of newsletters](#).

#### **Does the online service send push notifications?**

Push notifications are messages that are sent to your device and prioritized there. This online service uses push notifications in the state of delivery, if you have given your consent during installation or first use (Art. 6 para. 1a GDPR). You can disable the receipt of push notifications at any time in the settings of your device. Processing is carried out by the processors [360Dialog](#) and [MoEngage](#).

#### **Data control for the social media plug-ins used or links to social media platforms.**

Some pages contain buttons from social media networks (such as Facebook, Google, Instagram, X [Twitter], Pinterest, TikTok, Xing or LinkedIn) with which you can recommend the offers of Telekom Deutschland GmbH to your friends and acquaintances. To ensure that you have full data control, the buttons used only establish direct contact between the respective social network and the visitor when you actively click on the button (1-click solution). By activating the social media plug-in or link via the pictogram, also for sharing content, (Art. 6 para. 1 a GDPR), the following data can be transmitted to the social media providers: IP address, browser information, operating system, screen resolution, installed browser plug-ins, previous page if you followed a link (referrer), the URL of the current page, etc. The next time you open the website, the social media plug-ins are again provided in the preset inactive mode, so that no data is transmitted when you visit them again. Further information on social media plug-ins, the scope and purposes of the respective data processing as well as other data protection-relevant information can be found in the data protection declarations of the respective controller and for the explanation of the [1-click solution on Heise.de](#).

#### **Who or what is Utiq?**

##### About the Utqi Service

Utiq SA/NV ("Utiq") is a European AdTech company. Supported by several telecommunications network operators, Utiq operates a so-called Authentic Consent Service ("Utiq Service") for responsible digital marketing. The Utiq Service provides you with greater control and transparency over the use of your data when you consent to personalized experiences or analytics on Utiq's

partner websites. As part of the Utqi service, you will have access to a central data protection self-administration portal, the so-called Utqi [consenthub](#). There you can manage your preferences for the Utqi Service and your Utqi consents and exercise your data protection rights. All in one place and at any time.

#### About our partnership with Utqi

Telekom Deutschland GmbH provides the network-based infrastructure for this service. This means that if you give your active consent on a participating website, your IP address will be forwarded to us. This is used to check whether the requirements for using the service are met and, if applicable, to assist with the activation of the Utqi service. As part of the activation process, we compare your IP address with your mobile phone contract to generate a pseudonymous identifier known as a **network signal**. The **network signal** is created with the help of a secure procedure (e.g. encryption). This protects their identity before the **network signal** is forwarded to Utqi. Utqi uses this signal as part of its so-called **consentpass** system. In this way, Utqi helps participating advertisers and media companies to offer a personalized experience on their websites or to create analyses. At the same time, you as a user retain control over your data. The **Network Signal** is not enriched with your customer, internet usage or traffic data or other information. Nor do we create profiles about your behavior on individual websites. Data processing by us only takes place if you have given your consent for the stated purpose on the respective partner website. As a Telekom Deutschland GmbH customer, you can use the Utqi service on Utqi's partner websites when you visit them. The use of the service is only possible after prior, voluntary, and explicit consent (so-called opt-in procedure), as the Utqi service is inactive by default. Please note that consent must be given separately on each participating partner website.

#### How to manage your Utqi service

Through the Utqi [consenthub](#), you can view and manage your Utqi consents, revoke any consents you have given, deactivate the service or prevent its activation at any time. If you revoke your consent there, this also means that you revoke your consent to data processing by Telekom Deutschland GmbH. For more information about the Utqi Service, please visit the Utqi [consenthub](#) or [Utqi's Privacy Policy](#).

#### **Is my usage behavior evaluated, e.g. for advertising or tracking?**

We want you to enjoy using our digital services and using our products and services. For you to find the products that interest you and for us to be able to design our digital service in a user-friendly manner, we analyze your usage behaviors in a pseudonymized manner. Within the framework of the legal regulations, usage profiles are created. In the following, we provide you with general information about the various purposes of the processing. Via the "Consent to data processing" query, which appears when you access our digital service, you have the option of consenting to the processing or rejecting it in part or in full. Processing that is necessary for the provision of the digital service (see explanation above under section "What data is collected...") cannot be refused.

#### **a) Required processing**

##### Required functional

This processing is necessary to enable you to navigate through the Digital Service and use essential features. They enable basic functions such as order processing in the online shop and access to secure areas of the digital service. In addition, they serve the anonymous evaluation of user behavior, which we use to continuously develop our digital service for you. The legal basis for this processing is §25 para. 2 no. 2 TDDDG, Art. 6 para. 1b GDPR or, in the case of third countries, Art. 44 et seq. GDPR.

Company	Purpose	Storage period	Country
<a href="#">Telekom</a>	Shopping cart	Session, 30 days	Germany
<a href="#">Telekom</a>	Login incl. "Remember username" / "Stay logged in"	Session, 6 months (stay logged in)	Germany
<a href="#">Tealium</a>	Tag Management	3 month	Netherlands
<a href="#">PurpleView</a>	Video-Ident	12 hours	Germany
<a href="#">Risk.Ident</a>	Fraud prevention	Code-Snippet	Germany

#### **b) Optional processing**

This processing is used when you use additional features, such as chat. The possible functions are explained in the section "What data is collected, how is it used and how long is it stored?" of this Privacy Notice. The legal basis for this processing is §25 para. 1 TDDDG, Art. 6 para. 1a GDPR or, in the case of

third countries, Art. 49 para. 1a GDPR.

Company	Purpose	Storage period	Country
<a href="#">Genesys</a>	Text Chat Session		Deutschland
<a href="#">SurveyMonkey</a> (vorm. Usabilla)	Customer feedback	24 months	Ireland
Telekom	Chatbot (Frag Magenta)	14 days	Germany
<a href="#">MoEngage</a>	Push Notifications	24 months	Germany, USA
<a href="#">360Dialog</a>	Push Notifications	24 months	Germany
<a href="#">Salesforce Survey</a>	Service-Portal	6 months	Germany, France

Company	Purpose	Storage period	Land
<a href="#">Genesys</a>	Text Chat	Session	Germany
<a href="#">SurveyMonkey</a> (formerly Usabilla)	Customer feedback	24 months	Ireland
Telecom	Chatbot (Frag Magenta)	14 days	Germany
<a href="#">MoEngage</a>	Push Notifications	24 months	Germany, USA
<a href="#">360Dialog</a>	Push Notifications	24 months	Germany
<a href="#">Salesforce Survey</a>	Service-Portal	6 months	Germany, France
<a href="#">PurpleView</a>	Video-Outfit	12 hours	Germany

#### **c) Analytical processing**

This processing helps us to better understand usage behaviors. Analytical processing enables the collection of usage and recognition possibilities by first or third-party providers, in pseudonymous usage profiles. For example, we use analytical processing to determine the number of unique users of the Digital Service or to collect technical information in the event of a Digital Service crash, as well as to analyze user behavior based on pseudonymous information about how users interact with the Digital Service. The legal basis for this processing is Art. 6 para. 1a GDPR or, in the case of third countries, Art. 49 para. 1a GDPR.

Company	Purpose	Storage period	Country
<a href="#">Telekom</a> or <a href="#">Mapp</a> (vorm. Webtrekk)	Needs-based design and analysis	6 months	Germany
<a href="#">Adjust</a>	Needs-based design	30 days	Germany
<a href="#">Ipsos</a> (vorm. GfK)	Market research	Session	Europe

<a href="#">INFOline</a>	Reach measurement	60 days	Europe
<a href="#">Artefact</a> (vorm. Metalyzer)	Affiliate	30 days	Germany
<a href="#">Mapp</a> (vorm. Teradata)	Newsletter (Affiliate)	30 days	Germany
<a href="#">Matomo</a> (vorm. Piwik)	Needs-based design	13 months	Germany
<a href="#">AB Lyft</a>	A/B Testing	3 months	Germany
<a href="#">AT-Internet</a> (Xiti)	Needs-based design	6 months	Europe
<a href="#">Verint</a>	User surveys	24 months	Germany, Netherlands

**d) Services from other companies (independent third-party providers)**

This processing is used to be able to show you personalized and thus relevant advertising content.

Marketing processing is used to display interesting advertising content and to measure the effectiveness of our campaigns. This is not only done in Deutsche Telekom's digital services, but also in other digital services (third-party providers). This is also known as retargeting. It is used to create pseudonymous content or ad profiles, serve relevant advertising on other digital services, and derive insights about audiences who viewed the ads and content. Marketing and retargeting processing helps us to display relevant advertising content for you. By suppressing marketing processing, you will continue to see the same number of advertisements, but they may be less relevant to you. The legal basis for this processing is §25 para. 1 TDDG, Art. 6 para. 1 a GDPR or, in the case of third countries, Art. 49 para. 1 a GDPR.

Company	Purpose	Storage period	country
<a href="#">Telekom</a>	Needs-based design, advertising	24 months	Germany
<a href="#">Ad4Mat</a>	Advertising	24 months	Germany
<a href="#">Adform</a>	Advertising	60 days	Europe
<a href="#">AWIN</a>	Advertising	24 months	Germany
<a href="#">Mapp</a> (vorm. Webtrekk)	Marketing, (Personalization)	6 months	Germany
<a href="#">emetria</a> (vorm. Xplosion)	Profiling, advertising	12 months	Germany
<a href="#">Linkster</a>	Advertising	30 days	Germany
<a href="#">Trbo</a>	Personalization	24 months	Germany
<a href="#">Telekom</a>	Personalization	4 months	Germany
<a href="#">360Dialog</a>	Advertising	24 months	Germany

**e) Services from other companies (independent third-party providers)**

We have integrated third-party services that provide their services on their own responsibility or under joint responsibility with Deutsche Telekom. When you use our digital service, data is collected by means of cookies or similar technologies and transmitted to the respective third party, in some cases for Deutsche Telekom's own purposes. The legal basis for this data processing is Art. 6 para. 1 a and Art. 49 para. 1a GDPR. For information on further processing for the third-party provider's own purposes, please refer to the third-party provider's data protection information (purposes, storage period and legal basis). If data processing is also carried out under the joint responsibility of Deutsche Telekom, we provide information about the possible risks as follows.

Third country	Receiver	Data Types	Possible risk
United States of America (Data exporter: Google Ireland)	Google LLC	Usage data	EU-US Data Privacy Framework ensures an adequate level of data protection for

			data processing in the USA
Vereinigte Staaten von Amerika (Daten-exporteur: LinkedIn Irland)	LinkedIn Inc.	Usage data	EU-US Data Privacy Framework ensures an adequate level of data protection for data processing in the USA
United States of America (Data exporter: Meta Ireland)	Meta Platforms Inc.	Usage data	EU-US Data Privacy Framework ensures an adequate level of data protection for data processing in the USA

**Google**

**Google Ads:** In our online service, we use the **Google Ads** and **Floodlight** function of Google Ireland Ltd., Gordon House, Barrow Street, Dublin 4, Ireland ("Google"). This feature is used to present interest-based ads to visitors as part of the Google Network. In the digital service, the visitor can then be presented with advertisements that refer to content that the visitor has previously accessed in other digital services that use Google's remarketing function. If you still do not want Google's remarketing function, you can deactivate it by making the appropriate settings under <http://www.google.com/settings/ads>. Alternatively, you can opt out of the use of interest-based advertising through the Ad Network Initiative by following the instructions under [http://www.networkadvertising.org/managing/opt\\_out.asp](http://www.networkadvertising.org/managing/opt_out.asp). Further information on Google Ads and Google's privacy policy can be found at: <https://policies.google.com/technologies/ads?hl=de/>.

If you have reached our digital service via a Google ad, Google Ads will store a cookie on your device. This cookie expires after 90 days. The information obtained with the help of this so-called conversion cookie is used to compile statistics on our conversion rate. This means that we learn how many users have come to our websites through a Google ad and purchase a product within 90 days. If you do not wish to participate in the tracking process, you can disable cookies for conversion tracking by setting your browser settings to block cookies from the relevant domain: Google Ads: [googleadservices.com](http://googleadservices.com)

**Google YouTube Videos:** YouTube collects data to provide users with better services, from finding basic information, such as your language, to more complex issues, such as advertising. The information YouTube collects and how it is used depends on how you use the Services and how you manage your privacy settings.

If you're not signed in to a Google Account, the data collected is stored with unique identifiers associated with the browser, app, or device. For example, it can be used to ensure that language settings are retained throughout all sessions.

If you're signed in to a Google Account, data is also collected that is stored in your Google Account and is considered personal data. For more information, please visit: <https://policies.google.com/privacy?hl=de&q=de>

**Meta/Facebook**

We use the Meta pixel and the Customer Audience service in our digital service to optimize our advertising offer, if you have given Meta your consent to do so. Further information about these Meta Services and the privacy notice of Meta Platforms Ireland Ltd., Merrion Road, Dublin 4, D04 X2K5, Ireland ("Meta") can be found at the link

<https://www.facebook.com/privacy/explanation>.

If you use a Facebook user account, this can be recognized by the Meta pixel in our online service by the Facebook cookie set, via which the collected usage data is transmitted to Meta for analysis and marketing purposes. You can check and/or deactivate this data collection and the further processing and use of the data by Meta directly.

The meta pixel is a JavaScript code that transmits the following data to Meta:

- HTTP header information (including IP address, web browser information, location, document, URL of the online service and user agent, and day and time of use)
- Pixel-specific data; this includes the pixel ID and Facebook cookie data, including your Facebook ID (this data is used to associate events with a specific Facebook ad account and associate them with a Facebook user)
- Additional information about visiting our digital service, as well as standard and custom data events.



- Orders placed (purchases)
- Completion of registrations and trial subscriptions
- Searched products, access to product information.

The data processing only applies to users who have an account with Facebook or have accessed a Facebook partner page (whereby a cookie has been set). The display of advertising on Facebook (partner) pages using the "Customer Audience" service does not affect users who are not members of Facebook. If the Facebook ID contained in the Facebook cookie can be assigned to a Facebook user, Meta will assign this user to a target group ("Custom Audience") based on the rules we have determined, if the rules are relevant. We use the information obtained in this way for the presentation of Telekom advertising on Facebook (partner) pages. If you want to contradict the use of the Meta Pixel, you can set an opt-out cookie on Facebook or deactivate JavaScript. For more information and the setting options to protect your privacy for advertising purposes, please refer to Meta's privacy policy, which can be found on [https://www.facebook.com/ads/website\\_custom\\_audiences/](https://www.facebook.com/ads/website_custom_audiences/), among other places.

#### X (formerly Twitter) for Internet data

Twitter content is integrated into some digital services. These can be, for example, the embedded timeline or Twitter buttons. When you view such a page, [X \(formerly Twitter International Company\)](#), One Cumberland Place, Fenian Street Dublin 2, D02 AX07 Ireland may receive log data that contains data from the digital service you visit. This information is used to improve the use of the Digital Services, to protect the security and integrity of the Platform, and to display more relevant content, including ads. No connection is made between your activity and your name, email address, phone number, or username, and deletion, obfuscation, or aggregation is done after a maximum of 30 days. There is no collection of this data, which is located in the European Union. X [Twitter]'s Privacy Policy: <https://twitter.com/de/privacy>.

#### Twitter

The re-targeting and conversion tracking of [LinkedIn Ireland Unlimited Company](#) (Wilton Plaza, Wilton Place, Dublin 2, Ireland) by means of the LinkedIn Insight Tag enables the collection of statistical, pseudonymous data (referrer URL, IP address (shortened), device and browser characteristics) via the LinkedIn Insight Tag. In addition, this information is used to be able to display interest-specific and relevant offers and recommendations after you have taken an interest in certain products, information and offers on our online service. This information is stored in a cookie for 6 months. You can find out about the data processing by LinkedIn at any time under <https://www.linkedin.com/legal/privacy-policy?trk=registration-footer-privacy-policy> and object to it or revoke your consent via the cookie settings. Telekom Deutschland GmbH and LinkedIn are joint controllers for this processing in accordance with Art. 26 GDPR. If you have any questions, you can contact [datenschutz@telekom.de](mailto:datenschutz@telekom.de).

#### emetriq GmbH

emetriq is a provider of targeting services in the field of online marketing of advertising space. Targeting stands for a precise target group approach in online marketing and personalization of content. For this purpose, emetriq operates a data pool whose goal is to significantly increase the quality of targeting so that advertisers can display relevant advertising according to your interests. To enable user-specific advertising and content to be displayed, [emetriq GmbH](#) (Vorsetzen 35, 20459 Hamburg) collects information about surfing behaviors and app use. Cookies, measurement pixels, APIs or SDKs are used that can collect or process the following information:

- Pseudonym IDs: Cookie-ID, Identifier for Advertising (IDFA) oder Advertisings-ID (AdID), IP-Adresse
- App or browser information, such as browser identifier, time zone, language, operating system
- Information about seen or clicked advertising banners
- URL of the pages visited by our connected marketers
- Socio-demographic data, such as age decades, salutation, and abbreviated zip code
- Hashed login data (e-mail)

The collected data is pseudonymised at the earliest possible time either in the app or in the user's browser or in the first processing system and only then further processed. All information collected about a user is stored exclusively with the help of pseudonymous IDs. emetriq deletes this data after 6 months at the latest.

To enable cross-device personalization of advertising, emetriq assigns an identifier (ID) to each of your devices using your hashed email address. This makes it possible to assign the different assigned IDs to each other in cases where you have logged in to digital services using different devices. The involvement of a neutral authority, the so-called trusted third party, ensures that emetriq does not gain access to the email address. In individual cases, this makes it possible to assign a device to a user across providers, even if the user has not logged into the Telekom online service with his or her

device. This makes it possible to adjust the offer in line with your interests even without a login.

Telekom Deutschland GmbH and emetriq GmbH are joint controllers for this processing in accordance with Art. 26 GDPR. If you have any questions, you can contact [datenschutz@telekom.de](mailto:datenschutz@telekom.de).

Limited to the above-mentioned purposes, this data is also processed independently by emetriq and its technology partners. For more information, please contact emetriq: <https://www.emetriq.com/datenschutz>. In addition, emetriq works with the provider [The Trade Desk Ltd. UK](#) (abbreviated "TTD", in 1 Bartholomew Cl, London EC1A 7BL, United Kingdom). The Trade Desk processes the IP address and usage data (such as pages accessed and products). For this purpose, users are assigned a randomly generated ID by means of a cookie, which can be used to recognize the user in our online service as well as the online services of third parties in TTD's advertising network and to optimize advertising campaigns. Information on data protection at The Trade Desk can be found at <https://www.thetradedesk.com/us/privacy>

#### Deep Media

We use the Deep Media Advertiser Tag on our digital service, a service of [Deep Media Technologies GmbH](#) (Hohe Bleichen 8, 20354 Hamburg). The Deep Media Advertiser Tag is a tag management system for managing technology for marketing and optimization purposes. In particular, it is used to serve ads that are relevant and interesting to you and to improve campaign performance reports. When the advertiser tag is used, information is processed, for example in the form of cookies or click IDs. The processing of the data and, if necessary, the forwarding of these online identifiers by Deep Media Technologies GmbH is only carried out to providers for whom the user has given consent within the framework of the data protection settings. The collection and storage of data can be objected to at any time with the respective provider. Further information on the handling of data and opt-out options can be found in the respective sections of the providers in this privacy policy. Further information on the use of data by Deep Media Technologies GmbH can be found on the following website of Deep Media Technologies GmbH: <https://www.deepmedia.de/datenschutzerklaerung-advertiser-tag/>

#### Adform

In our digital service, we use the service of [Adform A/S](#) (Silkegade 3B, ST. & 1., 1113 Copenhagen, Denmark) to obtain evaluations of the performance of our campaigns, targeting data and advertisements, comparing the following:

- Cookie ID, 1st Party ID, Partner ID, Cross-Device ID oder Mobile Advertising ID
- Device information (browser type & settings, operating system)
- interactions, as well as
- approximate geographic location based on the truncated IP or GPS data

Adform analyzes the data collected via cookies and IDs to be able to serve interest-based advertisements. This information is stored for a maximum of 13 months, cookie-based information for 60 days. You can inform yourself about the data processing by Adform at [any time](#) under <https://site.adform.com/de/privacy-center/platform/datenschutzrichtlinie-fuer-produkte-und-services/#WiewirCookiesverwenden> and object to it or revoke your consent via the cookie settings.

Telekom Deutschland GmbH and Adform A/S are joint controllers for this processing in accordance with Art. 26 GDPR. If you have any questions, you can contact [datenschutz@telekom.de](mailto:datenschutz@telekom.de).

Privacy settings: You can revisit your [settings](#) at any time to manage your preferences.

#### Where can I find the information that is important to me?

Additional information on data protection when using our products, in particular for purposes of use, deletion periods, etc., can be found in the data protection information for the respective product under and <http://www.telekom.de/datenschutzhinweise> and under [www.telekom.de/datenschutz](http://www.telekom.de/datenschutz).

#### What rights do I have?

You have the right to:

- request information** on the categories of data processed, purposes of processing, any recipients of the data, the planned storage period (Art. 15 GDPR);
- request the **correction** or completion of incorrect or incomplete data (Art. 16 GDPR);
- revoke any consent given at any time with effect for the future (Art. 7 para. 3 GDPR);
- object to data processing that is to be carried out based on a legitimate interest on grounds relating to your particular situation (Art. 21 para. 1 GDPR);
- in certain cases, within the framework of Art. 17 GDPR, **to request the deletion** of data - in particular if the data is no longer necessary for

- the intended purpose or is unlawfully processed, or you have revoked your consent in accordance with above (c) or have declared an objection in accordance with above (d);
- f) to demand the restriction of data **under certain conditions** if deletion is not possible or the obligation to delete is disputed (Art. 18 GDPR);
  - g) data **portability**, i.e. You can receive your data that you have provided to us in a common machine-readable format such as z.B. CSV and, if necessary, transmit it to others (Art. 20 GDPR;)
  - h) complain to the competent **supervisory authority** about data processing (for telecommunications contracts: Federal Commissioner for Data Protection and Freedom of Information; in addition: State Commissioner for Data Protection and Freedom of Information of North Rhine-Westphalia).

**To whom does Deutsche Telekom pass on my data?**

**To processors**, i.e. companies that we commission to process data within the framework provided for by law, Art. 28 GDPR (service providers, vicarious agents). Deutsche Telekom remains responsible for the protection of your data in this case. In particular, we engage companies in the following areas: IT, sales, marketing, finance, consulting, customer service, human resources, logistics and printing.

**To cooperation partners** who provide services for you or in connection with your Telekom contract on their own responsibility. This is the case if you commission the services of such partners from us or if you consent to the involvement of the partner or if we involve the partner based on a legal permission.

**Due to legal obligation:** In certain cases, we are legally obliged to transmit certain data to the requesting government body.

**Where is my data processed?**

Your data will be processed in Germany and other European countries. In some cases, your data will also be processed in countries outside the European Union (i.e. in so-called third countries), currently for example: Storing/hosting of customer data (excluding traffic data) by Amazon Web Services EMEA SARL, Microsoft Ireland Operations Ltd., Google Cloud EMEA Limited, Ireland, and Salesforce.com Germany GmbH in Europe. Only administrator access within the framework of technical support is possible from the USA.

In addition, if data processing takes place in third countries, this will take place if you have expressly consented to this or if it is necessary for our provision of services to you or if it is provided for by law (Art. 49 GDPR). Your data will only be processed in third countries if certain measures are taken to ensure that an adequate level of data protection exists (e.g. adequacy decision of the EU Commission or so-called appropriate safeguards, Art. 44 et seq. GDPR).

**Who is responsible for data processing? Who is my contact person if I have questions about data protection at Deutsche Telekom?**

The data controller is Telekom Deutschland GmbH, Landgrabenweg 151, 53227 Bonn, Germany. If you have any questions, you can contact our [customer service](#) or our data protection officer, Dr. Claus D. Ulmer, Friedrich-Ebert-Allee 140, 53113 Bonn, [datenschutz@telekom.de](mailto:datenschutz@telekom.de).

Status of the data protection notice October 2024