

## Data privacy information

### General provisions

Deutsche Telekom AG, Technology & Innovation attaches great importance to protecting your personal data. We always inform you about personal data that we collect during your visit to our websites, how it is used and how you can influence the process. This data privacy information provides answers to the most important questions.

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

This data privacy information provides an overview of the items which apply to Deutsche Telekom processing your data in this web portal.

Further information, including information on data protection for specific products, is available at <https://www.telekom.com/en/corporate-responsibility/data-protection-data-security/data-protection>.

#### 2. Who is responsible for data processing? Who should I contact if I have any queries regarding data privacy at Deutsche Telekom?

Deutsche Telekom AG, Friedrich-Ebert-Allee 140, 53113 Bonn, Germany, acts as the data controller. If you have any queries, please contact our Customer Services department or the Group Data Privacy Officer, Dr. Claus D. Ulmer, Friedrich-Ebert-Allee 140, 53113 Bonn, Germany [datenschutz@telekom.de](mailto:datenschutz@telekom.de).

#### 3. What rights do I have?

You have the right

- a) to request **information** on the categories of personal data concerned, the purpose of the processing, any recipients of the data, the envisaged storage period (Art. 15 GDPR);
- b) to request incorrect or incomplete data is rectified or supplemented (Art. 16 GDPR);
- c) to **withdraw** consent at any time with effect for the future (Art. 7 (3) GDPR);
- d) to **object** to the processing of data on the grounds of legitimate interests, for reasons relating to your particular situation (Art 21 (1) GDPR);
- e) to request the **erasure** of data in certain cases under Art. 17 GDPR – especially if the data is no longer necessary in relation to the purposes for which it was collected or is unlawfully processed, or you withdraw your consent according to (c) above or objected according to (d) above;
- f) to demand under certain circumstances the **restriction** of data where erasure is not possible or the erasure obligation is disputed (Art. 18 GDPR);
- g) to **data portability**, i.e. you can receive your data which you provided to us, in a commonly used and machine-readable format, such as CSV and can, where necessary, transmit the data to others (Art. 20 GDPR);
- h) to **file a complaint** with the competent supervisory authority regarding data processing (for telecommunications contracts: the German Federal Commissioner for Data Protection and Freedom of Information (Bundesbeauftragte für den Datenschutz und die Informationsfreiheit); for any other matters: State Commissioner for Data Protection and Freedom of Information North Rhine-Westphalia (Landesbeauftragter für den Datenschutz und die Informationsfreiheit Nordrhein-Westfalen).

#### 4. Who does Deutsche Telekom pass my data on to?

**To processors**, i.e. companies we engage to process data within the legally defined scope, Art. 28 GDPR (service providers, agents). In this case, Deutsche Telekom also remains responsible for protecting your data. We engage companies particularly in the following areas: IT, sales, marketing, finance, consulting, customer services, HR, logistics, printing.

**To cooperation partners** who, on their own responsibility, provide services for you or in conjunction with your Deutsche Telekom contract. This is the case if you contract with us services from these partners or if you consent to the incorporation of the partner or if we incorporate the partner on the basis of legal permission.

**Owing to legal obligations:** In certain cases, we are legally obliged to transfer certain data to the requesting state authority.

We do not pass on your data to third parties for any other purpose, unless you have given express permission for us to do so or this is permitted by law.

## 5. Where is my data processed?

In general, user data is processed in the European Union. If your data is also processed in countries outside the European Union (i.e. in third countries) by way of exception, this is done only if you explicitly give your consent, or it is prescribed by law (Art. 49 GDPR). Furthermore, your data is only processed in third countries if certain measures ensure a suitable level of data protection (e.g. EU Commission's adequacy decision or suitable guarantees, Art. 44 ff. GDPR).

## 6. What data is recorded, how is it used and how long is it stored?

**Project data:** Deutsche Telekom collects the performance metrics regarding users' projects upon user's explicit permission by acceptance of Terms & Conditions. The project data is used for the purpose of improving the IoT Solution Optimizer web service, as well as in trend analyses of M2M or IoT product designs, or their aspects. The analysis algorithms do not include any private data associated with your user accounts or their association to project data.

Upon the expiration or deletion of the user's account, the personal data is automatically erased from the system and the project data is being anonymized. It not possible to correlate anonymized data to a specific user account. By default, your anonymized project data is archived for a period of four years, after which it is finally purged automatically by the system.

**Personal data:** Data such as contact details, being your name, e-mail, postal address, company name are collected for the users who have registered to the IoT Solution Optimizer for the purpose of using the service. These data are collected directly from the users upon registration and completion of the user profile and are solely used for access to the service and user administration purposes.

**Web contact forms:** Data such as name, e-mail, postal address, company name are collected from user who voluntarily requested support or information on particular components of the service and are used solely for the purpose of processing the request and providing the support.

## 7. How secure is my data?

We have taken extensive technical and operational security precautions under German law to protect your data against unauthorized access and misuse.

## 8. Data control for the social media plug-ins used

The web portal of the IoT Solution Optimizer does not use social media plug-ins.

When the social media plug-in is activated (Art. 6 (1) a GDPR), the following data can be forwarded to the social media provider: IP address, browser information, operating system, screen resolution, installed browser plug-ins (such as Adobe Flash Player), previous website if you followed a link (referrer), URL of the current website, etc.

## 9. Will my usage habits be evaluated, e.g. for advertising purposes, tracking or fraud prevention?

### Explanations and definitions

We want you to enjoy using our website and take advantage of our products and services. We have a business interest in ensuring this is the case. We analyze your usage habits on the basis of anonymized or pseudonymized data so you can find products that interest you more easily and so that we can make our website more user-friendly. We or companies commissioned by us to process data create usage profiles to the extent permitted by law. This information cannot be traced back to you directly. Subsequently we inform you generally about the various purposes and techniques. Afterwards you have the right to revoke your consent. However, please remember that in this case you may not have access to the full range of functions offered by our websites.

### a) Purposes (Art. 6 (1) f GDPR / §15 (3) German Telemedia Act (Telemediengesetz – TMG)

#### Tag management

Tag management is used to manage tracking tools in websites. A tag is set for each page to do this. Based on the tag, the system can determine which tracking tools should be used for this page. Tag management can be used to specifically control tracking so that the tools are only used where appropriate.

#### Market research / Reach measurement

Reach measurement provides statistics on a website's usage intensity and the number of users, along with comparable figures for all the connected services. Individual users are not identified at any time. Your identity is always protected.

### b) Techniques

#### Cookies

We use cookies for certain services. These are small text files that are stored on your computer. They enable the system to tell if you repeatedly visit websites from the same computer.

**Session cookies** are cookies which are only stored on your computer for the duration of your Internet session and are required for transactions (e.g. to log in or to complete a purchase). They simply contain a transaction ID.

For certain services, we use persistent cookies, which are stored on your computer for future sessions. In this case, we notify you about the cookie's storage period.

You can set your browser to prevent these cookies being stored or to delete the cookies at the end of your Internet session. However, please remember that in this case you may not have access to the full range of functions offered by our websites. For information about browser settings go to: <https://www.sicherdigital.de/sicher-surfen#sicher-surfen-browsereinstellungen>

### JavaScript

JavaScripts are used to call the application and to transfer the collected parameters to the particular service provider/measurement pixel provider.

AspNet.Consent – Consent feature allows you to ask for (and track) consent from your users for storing personal information:

<https://docs.microsoft.com/en-us/aspnet/core/security/gdpr?view=aspnetcore-2.2>

.AspNetCore.Antiforgery – Prevent Cross-Site Request Forgery (XSRF & CSRF) attacks

<https://docs.microsoft.com/en-us/aspnet/core/security/anti-request-forgery?view=aspnetcore-2.2>

.AspNetCore.Identity.ApplicationCore Identity – Allows you to add login features to your application and makes it easy to customize data about the logged-in user.

<https://www.nuget.org/packages/Microsoft.AspNetCore.Identity/>

.AspNetCore.Mvc.CookieTempDataProvider – Storing temp data which are not permanent (used only in some cases)

.AspNetCore.Session ASP.NET Core maintains session state by providing a cookie to the client that contains a session ID, which is sent to the app with each request.

<https://docs.microsoft.com/en-us/aspnet/core/fundamentals/app-state?view=aspnetcore-2.2>

ARRAffinity Affinity Cookies are used to aid people who need to stay with a certain instance of web app or web site in Azure. The reason for this is that we strive for statelessness, but do not always achieve it. This means that the user must stay on the particular instance that they using till they break state and then things are saved at that time.

<https://blogs.msdn.microsoft.com/devschool/2015/06/19/azure-arraffinity-makes-affinity-cookies/>

Identity.External authentication handlers for external providers

<https://docs.microsoft.com/en-us/aspnet/core/security/authentication/social/?view=aspnetcore-2.2&tabs=visual-studio>

Identity.TwoFactorUserId – This cookie is used during the two-factor authentication procedure.

## 10. Will my usage habits be evaluated, e.g., for advertising purposes?

We do not evaluate usage habits for commercial purposes.

## 11. Services from other companies that assume responsibility for providing their services

You can consult further information on cookies and the individual providers on the websites [www.meine-cookies.org](http://www.meine-cookies.org) or [www.youronlinechoices.com](http://www.youronlinechoices.com). Here you can also choose not to receive usage-based online advertising from a single or from all of these companies at <http://www.youronlinechoices.com/de/praferenzmanagement>.

## 12. Where can I find further information regarding data privacy at Deutsche Telekom?

Further information, including information on data privacy in special products, is available at <http://www.telekom.com/dataprotection>.

**13. Who should I contact if I have any queries regarding data privacy at Deutsche Telekom?**

If you have any queries, please contact our Customer Services department or the Group Data Privacy Officer at Deutsche Telekom AG, Dr. Claus D. Ulmer, Friedrich-Ebert-Allee 140, 53113 Bonn, Germany [datenschutz@telekom.de](mailto:datenschutz@telekom.de).

Data privacy information last revised: August 19, 2019