Data Privacy statement of Deutsche Telekom AG („Telekom“) for Love Magenta Connected Underwear App

General

Deutsche Telekom AG attaches great importance to protecting your personal data. We always inform you what personal data we collect, how your data is used, and how you can influence the process.

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 app.
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 and https://www.telekom.com/en/deutsche-telekom/privacy-policy-1744.

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

Deutsche Telekom AG 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.

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 (Bundesbeauftragter 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)

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. Example: Upon presentation of a court order, we are obliged under § 101 of the German Copyright Act (Urheberrechtsgesetz – UhhG) to provide the owners of copyrights/ancillary copyrights with information about customers who have allegedly offered copyrighted works via Internet file sharing

Where is my data processed?

In general, your data is processed in Germany and in other European countries.

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 have explicitly given your consent or it is required so we can provide you with services 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). .

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

If you are using the app our server will temporarily process the IP address of your device and other technical features such as viewed contents within the app (Art. 6 Abs. 1 b DSGVO).

Authorizations

For the app to work on your device, it needs access to various functions and data on the device. You need to grant certain authorizations to do so (Art. 6 (1) a GDPR).

The authorization categories are programmed differently by the various manufacturers. With Android for example, individual authorizations are grouped into authorization categories and you can only agree to the authorization category as a whole.

However, please remember that in the case of revocation you may not have access to the full range of functions offered by our app.
If you have granted authorizations, we will only use them to the extent described below:

:

Location data
The app requires information on your current location. In order to connect your LoveChip (Bluetooth beacon) with your app a Bluetooth connection is required, and Android only allows this connection if the App can determine your current location. The app will not detect your location and there will be no storage or processing of location data.

Does the app send push notifications?

Notifications are messages that the app sends to your device and that are displayed with top priority. This app uses local notifications by default, provided you have given your consent during the app installation or the first time you use the app (Art. 6 (1) a GDPR). You can deactivate receipt of notifications at any time in your device settings.

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

Explanations and definitions:

We want you to enjoy using our app and take advantage of our products and services. We have an economic interest in ensuring this is the case. We analyze your usage habits on the basis of anonymized or pseudonymized data so you can find the products that interest you and so we can make our app 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 app.

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 apps. A tag is set for each screen mask 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 aims to statistically determine an app's use intensity and the number of users as well as obtaining 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 the app from the same device.

Session cookies are cookies which are only stored on your device 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 device for future sessions. In this case, we notify you about the cookie's storage period.

Measurement pixels
Measurement pixels are simply images measuring 1×1 pixels. They are transparent or are the same color as the background, making them invisible. If an app page is opened that contains a measurement pixel, this small image is then downloaded from the provider's server on the Internet and the download is recorded on the server. This way the process provider can see when and how many users requested this measurement pixel or visited an app page. The provider can also record further information, such as browser information, operating system, screen resolution.

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

Variant 1: (individual opt-in / opt-out)
Processes used in this app:

Company	Purpose	Storage period	Involved as	Opt-in /opt-out
Adjust	Measurement of reach	1 month	Owner	[BUTTON]

Variant 2: (centralized opt-in / opt-out)
You can revoke data collection, processing and usage with the "Transfer pseudonymous usage data" button. Please note that only the usage analysis performed by this app will be disabled.

[BUTTON] Transfer pseudonymous usage data

Processes used in this app:

Company	Purpose	Storage period	Incorporated as
Adjust	Measurement of reach	1 month	[BUTTON]

Data privacy information last revised: 07/30/2019