Data Privacy Information – Corporate PKI (cPKI) of Deutsche Telekom AG

Contents

Change history/release notes

Version	Last revised	Author/editor	Changes/comments
1.0	Aug. 20, 2018	Deutsche Telekom Security	First Version
1.0	May. 20, 2019	Deutsche Telekom Security	annual review
2.0	July 01, 2020	Deutsche Telekom Security	Change Company name and annual review
3.0	Nov. 10, 2021	Deutsche Telekom Security	Annual review and correction of spelling mistakes
3.1	Nov. 28, 2022	Deutsche Telekom Security	Annual review, change of department name, change of Board of Management
3.2	Jan. 31, 2023	Deutsche Telekom Security	Review and QS
4.0	Feb. 01, 2023	Deutsche Telekom Security	Release
4.1	Feb. 20, 2024	Deutsche Telekom Security	annual review and QS
5.0	Feb. 23, 2023	Deutsche Telekom Security	Release

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

1. Who is responsible for data processing? Who should I contact if I have any queries regarding data privacy?

The party responsible for data privacy ("controller") is Deutsche Telekom IT GmbH, Landgrabenweg 151, 53227 Bonn, Germany. If you have any queries, please contact our Group Data Privacy Officer, Dr. Claus D. Ulmer, Friedrich-Ebert-Allee 140, 53113 Bonn, Germany, datenschutz@telekom.de.

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

The legal basis for processing your personal data is provided by Article 6 (1 letter b) GDPR and under German law in accordance with § 26 of the German Federal Data Protection Act, *(Bundesdatenschutzgesetz, BDSG* Data processing for employment-related purposes."

To be able to use the Corporate Private Key Infrastructure (cPKI) as an employee of the Deutsche Telekom AG Group, it is necessary to process the following data categories in the cPKI:

- Contact information (e.g., name, address). Only company contact data is processed, private contact data is excluded.
- Communication data (e.g., phone numbers, email addresses). Only company communication data is processed, private communication data is excluded.
- Identifier data (e.g., Corporate ID (CID), card numbers (MyCard))
- Certificate data (data on encryption, signature, and authentication certificates)
- verifiable logging data on certificate processes (issuance, renewal, revocation)
- general specific management data (e.g., IDs of internal/external employees, single-use passwords for certificate management)

Based on the statutory requirements of eIDAS (the **e**lectronic **I**dentification, **A**uthentication and trust **S**ervices Regulation), commissioned and identification data, particularly information on certificate applications, their validation, and the certificates and the revocations resulting therefrom must be retained for a period of seven (7) years after expiry of the certificates' validity.

3. To whom is my data disclosed?

As a rule, your personal data will not be passed on outside the Telekom Group unless this is required by law.

Disclosure based on a legal obligation:

The obligation not to disclose confidential information or personal data does not apply if disclosure of such information/data has been ordered by force of law or by a court ruling or an administrative authority or serves to implement legal judgments.

4. Where is my data processed?

Your data will be processed in Germany and other European countries.

5. What rights do I have?

You have the right

a) to request **information** about the categories of data processed, the purposes of processing, any recipients of the data, and the envisaged storage period (Article 15 GDPR);

b) to request that incorrect or incomplete data be **rectified** (Article 16 GDPR);

c) to **withdraw** consent at any time with effect for the future (Article 7 (3) GDPR)

d) to **object** to the processing of data on the grounds of legitimate interests, for reasons related to your particular situation (Article 21 (1), GDPR);

e) to request the erasure of data in certain cases under Article 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 in accordance with (c) above or object in accordance with (d) above

f) to demand under certain circumstances the **restriction** of data where erasure is not possible, or the erasure obligation is disputed (Article 18 GDPR)

g) to **data portability,** i.e., you can receive your data that you provided to us, in a commonly used and machine-readable format such as CSV, and can, if necessary, transfer the data to others (Article 20 GDPR;)

h) to file a complaint about the data processing with the responsible supervisory authority (state representatives for data privacy and freedom of information, North Rhine-Westphalia).