Privacy Policy for the use of the “easyPhone” app

1. Subject matter of this Privacy Policy

We appreciate your interest in our mobile application "easyPhone by TKS" (hereinafter referred to as "service"). The protection of your personal data ("data") is a special and important concern for us. Below, we would like to inform you about the data collected when using the service and how we use it. We would also like to inform you about the technical and organizational measures we have taken to protect your data. This Privacy Policy may be accessed at any time within the app via the navigation menu under “Privacy Statement”.

2. Controller and service provider

Responsible body within the meaning of the General Data Protection Regulation (GDPR), the German Federal Data Protection Act (“Bundesdatenschutzgesetz”, “BDSG”) and at the same time service provider within the meaning of the Telemedia Act (“Telemediengesetz”, “TMG”) is TKS Telepost Kabel-Service Kaiserslautern GmbH.

3. Your data

Personal data means any information relating to an identified or identifiable natural person, that is, details of your personal or material circumstances, such as your name, date of birth, or e-mail address.

4. Processing of your data

The app enables you to make and receive phone calls via a mobile application.

We process your data solely for the performance of our contracts to which you are subject. The purpose of processing your data is the proper provision of the service via the mobile application. Specifically, we provide the following services:

4.1 Login

In case you concluded a contract for the use of easyConnect you will automatically be provided with login data for the use of the services in the mobile app. You can download the app and use the service via mobile data network or WiFi by logging in with the login data provided.

4.2 Service related contract data

We use contract related data to determine which contract model and subscription mode you have chosen to provide the VoIP telephony service within the easyPhone App.

4.3 Mobile location information usage

We ask the location access permission only if the SIP account is configured to do so, and only in the following use cases:

- When the SIP account is used in a country with Dispatchable Location for emergency calls legal requirement.

In this situation, the app attempts to acquire your location information in case a call to an emergency number is placed. Please note that emergency calls are usually routed to your phone's native dialer instead of requesting location access. Please consult with support to learn how emergency calls are handled for your account.

- When the SIP account is configured to send location data during SIP registration

We will only use your Location information for the specific reason for which it was provided to us.

4.4 Adressbook

If you allow the usage of your phone address book in the contact settings menu we will use them to dial the phone numbers an also align incoming phone calls the names of callers if they are stored in your address book.
We use your contacts only within your device and do not forward the contacts to third parties.

4.5 Microphone

Your microphone is solely used for telephone calls.

4.6 Camera

To facilitate secure and user-friendly authentication, the app utilizes the mobile device’s camera exclusively for scanning a QR code. This QR code is provided to the customer as part of their contract confirmation documentation.

Upon scanning, the QR code transmits the credentials required to authenticate the customer within the app. These credentials are processed solely for the purpose of login and are not stored or retained beyond the authentication process. No personal data is permanently saved, and all transmitted information is discarded immediately after successful login.

The processing of data is strictly limited to what is necessary to enable authentication. The use of the camera and QR code functionality does not grant the app access to any other camera data or device content.

5. Duration of processing

In principle, we only process your data for as long as necessary for the provision of the performances within the service. For example, if you have deleted the service, we will also regularly delete your data. This is not the case if we are obliged to retain it due to statutory retention requirements, in particular for tax and balance sheet reasons. In this case we will delete your data at the end of the corresponding retention periods.

6. Data transfers to third parties

A transfer of data to third parties solely takes place in the case in which you have declared your express consent in advance or if we are entitled or obliged to do so by contract or by law or if we are legally obliged to do so. A transfer may be necessary if we commission companies such as technical service providers with the performance of corresponding services. In such a case, we have concluded respective data protection agreements with the service providers in order to legitimize and secure the transfer.

A transfer of your data to a third country outside the European Union or the European Economic Area or an international organization does not take place.

7. Cookies, analytics tools

The easyPhone app can send you notifications, for example incoming phone calls. We do not use cookies or analytics tools, except you have declared your express consent to TKS push notifications. All of your data will be collected and used solely for the purpose of fulfilling the functionality of the service.

To enable push notifications to be sent, a "Firebase installation IDs" is created, which uniquely identifies the app installation on your device. The ID is used to identify the message destination. The messages are sent via the Google Firebase Cloud Messaging service, which is offered by Google, Inc. Mountain View, USA. Further information on Google Firebase Cloud Messaging can be found at https://firebase.google.com/products/cloud-messaging/ and in Google's data protection declaration at http://www.google.de/intl/de/policies/privacy.

By agreeing to receive push notifications, you consent to the Firebase installation IDs being stored on our servers and used for sending. We assigned the installation IDs to the specific users, because personal messages are sent to them. The ID will be kept until it is revoked and only then will it be deleted from our servers. At Google, this token can still exist for up to 180 days.

You retain full control over the use of your data when using the service. If you decide to revoke your consent you can deactivate push notifications within the respective app menu.

8. Data Security

We use technical and organizational security measures to protect the data collected and processed, in particular against accidental or intentional manipulation, loss, destruction or against the attack of unauthorized persons. Our security measures are continuously improved in line with technological developments.

9. Data subject rights

You have the right to request information about the use of our service or to correct or delete your data. You may also claim a right of restriction of processing or of data portability. Finally, you have the right to complain to a regulator.

10. Contact

If you have any further questions or remarks regarding the subject of data protection or the exercise of your rights, you are welcome to contact our data protection officer:

TKS Telepost Kabel-Service Kaiserslautern GmbH
- Datenschutzbeauftragter -
Altes Forsthaus 2
67661 Kaiserslautern