Privacy Policy

Delavska hranilnica d.d. Ljubljana gives utmost importance to the protection of personal data of its users. This Privacy Policy determines the purpose and means of processing of personal data and describes how we collect, use, process, and disclose your data, including personal data in conjunction with your access to and use of DH Denarnik mobile wallet.

When this Privacy Policy mentions »we«, »us« or »our«, it refers to Delavska hranilnica d.d. Ljubljana, with seat and registered address at Miklošičeva cesta 5, 1000 Ljubljana, which is responsible for the processing of your data under this Privacy Policy (the »**Data Controller**«). For additional information with respect to personal data collection, processing and protection please contact: e-mail address dpo@delavska-hranilnca.si, phone number +386 1 3000 200.

When this Privacy Policy mentions »you«, »your« or »yours« it refers to you as the user of our Service.

For the purposes of this Privacy Policy the term „Service" consist of products, services, technologies, or functions, and all related applications and services offered to you through which we provide digitization and payment services.

By accepting Terms and conditions together with this Privacy Policy, you agree to the collection, use, process, storage and disclosure of data in accordance with this Privacy Policy. The personal data that we collect, use, process and storage is used only for providing and improving the Service. We will not use, share or disclose your personal data to any third party, except as described in this Privacy Policy.

1. What is the Legal basis for processing of data?

Processing is necessary for the performance of a contract to which the data subject (you) is a party and under which the Data Controller is obliged to provide services, such as registration of the mobile wallet, digitization of payment card and mobile payment services.

2. What data is being collected and/or processed?

DATA ABOUT YOU/YOUR DEVICE:

- Name and Surname
- Street and house number, Postal Code, City name
- Tax number
- Account data (IBAN and BIC)
- Telephone number
- Contact data (alias) information: phone number, email, contact data (alias) registry plate
- Wallet registration timestamp
- Last login into the wallet
- Terms and Conditions (together with this Privacy policy) acceptance timestamp
- Info about your mobile device: manufacturer, model, OS version, IMEI number, HW serial number
- Push token
- Transaction details

DATA ABOUT THE DIGITIZED CARD (for operating systems where this functionality is available):

- Name and surname of the owner of the card
- Type of the card (Mastercard, Maestro)
- Colour of the card
- Status of the card (active/deleted)
- Last 6 numbers of PAN
- Expiry date
- Unique identifier
- Token
- Info which is the default card
- Transaction details

STATISTICAL ANALYSIS OF DATA IN ANONYMOUS FORM

Described below are the data the mobile application collects for the purpose of statistical analysis with the help of third party service Firebase from Google. These data are in an anonymous form.

The following products from Firebase are used: Firebase Cloud Messaging, Firebase Crash Reporting, Firebase Crashlytics, Firebase Performance Monitor, Firebase Remote Config and Google Analytics for Firebase.

The type of information collected through the Google Analytics for Firebase includes:

- Number of users and sessions
- Session duration
- Operating systems
- Device models
- Geography
- First launches
- App opens
- App updates
- Android Advertising Identifier or Advertising Identifier for iOS

The type of information collected through the Firebase Performance Monitoring includes:

- General device information, such as model, OS, and orientation
- RAM and disk size
- CPU usage
- Carrier (based on Mobile Country and Network Code)
- Radio/Network information (for example, WiFi, LTE, 3G)
- Country (based on IP address)
- Locale/language
- App version
- App foreground or background state
- App package name
- An pseudonymous app-instance identifier
- Network URLs (not including URL parameters or payload content) and the following corresponding information:
    - Response codes (for example, 403, 200)
    - Payload size in bytes
    - Response times
- Duration times for automated traces.

In the case of an error in the app we collect data and information (through third party products mentioned in this paragraph) on your phone called Log Data. This Log Data may include information such as your device Internet Protocol ("IP") address, device name, operating system version, the configuration of the app when utilizing our Service, the time and date of your use of the Service, and other statistics.

For details how Firebase products collects and processes data, please see their Privacy policy at https://firebase.google.com/support/privacy/.

Document »How Google uses data when you use our partners' sites or apps« is accessible at https://policies.google.com/technologies/partner-sites.

By using our Service you consent to collection and processing of these data.

USE OF PERMISSIONS ON YOUR DEVICE

The mobile application requires access to the data and components of your device described below to function properly.

Permissions on Android device

Find accounts on the device
The mobile application requires access to accounts for reasons of compatibility.

Directly call phone numbers
The mobile application requires access to telephone calls for the purpose of calling the Data Controller's contact numbers and for sending messages to back-office systems for the digitisation of a specific card.

Read your contacts, modify your contacts (Contacts)
It is used to access your phone book to retrieve a contact data (alias) which is then translated to recipients account information.

Take pictures and videos (Camera)
The mobile application needs this to initiate a payment based on transaction data retrieved from QR.

Read phone status and identity
The mobile application requires this permission for security reasons.

View network connections, Full network access, View Wi-Fi connections and Receive data from the internet
The mobile application requires access to the internet to function.

Prevent device from sleeping
The mobile application requires access to this permission to prevent a device from switching to stand-by mode during the payment process.

Control vibration
The mobile application requires this permission to send feedback to you.

Use fingerprint hardware
If your device supports fingerprint recognition, the mobile application requires this permission for user authentication.

Modify or delete contents of your SD card and Read the contents of your SD card
The mobile application requires these two permissions to save data on a device.

Control Near-Field Communication
The mobile application requires access to communications using NFC technology for the purpose of communicating with POS terminals.

Pair with Bluetooth devices
This permission is requested by Mastercard to read an identifier for security aspects.

Read badge notifications
This permission is needed to allow to read and change number of notifications received by the mobile application.

Permissions on iOS device

Take pictures and videos (Camera)
The mobile application needs this to initiate a payment based on transaction data retrieved from QR.

Read your contacts, modify your contacts (Contacts)
It is used to access your phone book to retrieve a contact data (alias) which is then translated to recipients account information.

Use fingerprint hardware
If your device supports fingerprint recognition, the mobile application requires this permission for user authentication.

Face ID
If your device supports face recognition, the mobile application requires this permission for user authentication.

Read badge notifications
This permission is needed to allow to read and change number of notifications received by the mobile application.

Background application refresh
It is used to refresh the application while running in the background of the mobile device.

You can limit the access to your personal data in the mobile application through the settings of your mobile device. Please note that certain functions will be disabled if you limit access which might cause the mobile application not to function properly.

3. How we use the data we collect

We use, store, and process data, including personal data, about you and your device in order to provide the Service of:

- Verifying or authenticating information or identifications provided by you;
- Authenticating your access to the mobile application;
- Registering a digital wallet within the mobile application;
- Digitizing a payment card (create a token);
- Sending instant payments to the merchant via the QR interface;
- Sending instant payments to the merchant via the NFC interface (if the Mobile device so allows);

- Sending data for payment with digitalized card to merchant through NFC communication (if the mobile device so allows);
- Sending instant payments to the recipient who has a defined contact data (alias) in the Flik Directory;
- Sending request for payment to a recipient who has a defined contact data (alias) in the Flik Directory;
- Receiving instant payments;
- Receiving requests for payment;
- Viewing the status of transactions performed with the mobile application;
- Providing and monitoring your payment transactions;
- Enforcing our legal rights.

4. With whom we share the data

The mobile application does not share or disclose the data to any third parties, except the data needed for registration, digitization, payment and processing of transaction details as disclosed in this document.

Data are disclosed to Mastercard for Mastercard products. This is needed in order to generate a digitized card (create token) and map the token to an appropriate PAN.

Processing of data and payment transactions is carried out on behalf of us by a processor with whom we have entered into a legal contract and is therefore our contract partner for the processing of personal data. All applicable laws and regulations are considered in the processing of data.

For push notifications we use Firebase Cloud Messaging from Google. Please see the appropriate Privacy Policy at https://firebase.google.com/support/privacy/.

We don’t share analytical data with any third party except as noted in this document.

5. Push notifications and Opt-Out

Push notifications are used for sending conformations on received payments or request for payments. You may opt-out of receiving such notifications from the settings of the app and by going to your device Settings, clicking on App Notifications and then changing the settings.

6. Security

We take the responsibility to ensure that your personal data is secured.

To prevent unauthorized access to or disclosure of data transmitted, stored or otherwise processed we maintain physical, technical, electronic, organisational and procedural safeguards that comply with applicable regulations to guard non-public personal data. All internet communications are secured using all necessary measures. We allow access to your personally identifiable data only to persons authorised to process such data who need to know such information in order to provide the Service to you. Such persons are bound by obligation of confidentiality.

7. Changes to this Privacy Policy

We reserve the right to modify this Privacy Policy at any time in accordance with this provision. If we make changes to this Privacy Policy, we will post the revised Privacy Policy on our web site and in the mobile application and notify you.

For additional information regarding personal data collection, protection and processing, please read the document General information on the protection of personal data, available on www.delavska-hranilnica.si.

Ljubljana, 27th October 2020