Privacy Policy

Delavska hranilnica d.d. Ljubljana (»DH«) 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 connection 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 headquarters 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" refers to management of card settings, transactions review and payment history, authorization of e-commerce payments and adding cards to the mobile wallet of third-party providers[1] ("TPP") in accordance with the General Terms of payment service to use DH payment cards in mobile wallets from third-party providers ("Issuer Terms of TPP Services") and receiving instant payments in accordance with the rules of the Slovenian national Flik scheme and the General terms and conditions for using the DH Denarnik mobile wallet (»Terms and Conditions«).

By accepting Terms and conditions of mobile wallet DH Denarnik and/or Issuer Terms of TPP Services, 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 of data is necessary:

- for the performance of a contract (Article 6(1)(b) of the GDPR) concluded by the data subject (you) and under which the Data Controller is obliged to provide the services as defined in the Terms and Conditions;
- on the basis of your explicit consent (Article 6(1)(a) of the GDPR), as defined hereinafter (for instance, if you consent to receiving push notifications or explicitly consent to agree with Issuer Terms of TPP Services);
- on the basis of the requirements of the applicable legislation, namely the provisions of the Payment Services, Electronic Money Issuing Services and Payment Systems Act (hereinafter: ZPlaSSIED) and the Prevention of Money Laundering and Terrorist Financing Act (hereinafter: ZPPDFT-1) (Article 6(1)(c) of the GDPR).

[1] Mobile Wallet of Third-party Providers is a collective term for mobile wallets of third-party providers with which DH has concluded a mutual agreement to enable the cards to be added in their mobile application.

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

Data about you and your device, in the process of registration in the applicaton:

- Info about your mobile device:
- operating system and version,
- Tax number
- Name and Surname
- Mobile application and its version,
- IP address,
- Contact data (alias) information: phone number, email, contact data (alias) registry plate
- Type of user (natural person),
- Street and house number, Postal Code, City name
- Payment card number and its expiriy,
- Contact number for sending a one-time password.

Data about you and your device, when using Flik functionalities:

- Transaction account number (IBAN and BIC),
- Push token,
- Data about transactions.

Information about you and your mobile device, if you have added your DH payment card to the mobile wallet of a third-party provider with whom the savings bank has a partnership agreement:

- Push token (for sending payment tokens and push notifications),
- Amount and merchant name for online payments,
- Amount and merchant name for payment card transactions, executed with application,
- Payment card details (limits, security settings).

If you use the payment services in accordance with the Issuer Terms of TPP Services according to which you have added your DH payment card into TPP mobile wallet, DH exchanges with the third-party provider some of the personal data required to add the cards to the third-party mobile wallet and its use in the digitized form of a payment card. Third party mobile wallet providers are processing user information as independent data controllers. Before using the service, in the step before adding the card to the mobile wallet of the third-party provider, it is important to familiarize yourself in detail with their terms of service and information about the processing of personal data by the selected third-party mobile wallet provider.

DH exchanges the personal data of cardholders with third-party mobile wallet providers in order to allow the user to pay with a digitized DH payment card through the payment services of third-party mobile wallet providers.

Adding a card to Google Pay (Third-Party mobile provider):

In case of adding a card to the Google Pay service, the user adds his DH payment card to the Google Pay by selecting the "Add to Google Pay" button in the DH Denarnik mobile wallet. In the steps that follow, the user is redirected to the confirmation screen. At the user's request, DH provides his contact information and information about his DH payment card (“Provisioning Data") to Google Ireland Limited (hereinafter: "Google"), based in Ireland. DH as an Issuer provides Provisioning Data to Google Pay provisioning form and User explicitly consents before submitting it to Google Pay:

- First and Last Name,
- Billing Postal Code,
- Billing Street Address,

- Billing Country Code,
- Billing City,
- Full Phone Number,
- Opaque (i.e. encrypted) Payment Card,
- Funding Primary Account Number (i.e. fPAN),
- Expiration Date

Deleting your card from Google Pay

The user can remove the card from Google Pay and Google Wallet at any time by selecting the "Remove payment method" option under the selected digitized DH payment card (icon on the top right) in the Google Wallet settings.

Payment with Google Pay

When using your digitized DH payment card to make payments via Google Pay, DH shares encrypted data with Google about the payments that you, as the cardholder, make via the Google Pay. "Tokens" are used to authorize and execute payments, which, in accordance with the rules of the Mastercard card scheme, allow your personal information to remain confidential as it is encrypted during the payment process.

In order to prevent scams and fraud related to payment services in accordance with ZPlaSSIED and ZPPDFT-2, DH may receive data from Google regarding the cardholder's device, payments, location and account of the cardholder.

General information on how the savings bank processes personal data and information on the rights of individuals is available at https://www.delavska-hranilnica.si/o-hranilnici/predstavitev/varstvo-osebnih-podatkov.

Use of permissions on your device

The mobile application requires access to the data and components of your device described below for the proper functioning of some of its functions.

Required permissions to use the mobile application on Android device

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.

Disable stand-by mode
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.

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

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

Optional permissions to use the mobile application on Android devices:

Enable fingerprint authentication and biometrics
If your device supports fingerprint recognition or other biometric identification, the mobile application requires this permission for user authentication.

Photographs and camera
The mobile application needs camera access in order to scan a QR code and thus trigger payment.

Access Contacts, Edit Contacts
It is used to access the Contacts on your phone to obtain the recipient's contact information (alias), which is then translated into the recipient's account information.

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 digitization of a specific card.

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.

Overlay permission
A screen overlay allows making NFC payments outside the mobile application.

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

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

Required permissions to use the mobile application on iOS device

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.

Optional permissions to use the mobile application on iOS devices:

Photographs and camera
The mobile application needs camera access in order to scan a QR code and thus trigger payment.

Mobile data transfer
The mobile application requires access to the internet to function.

Access Contacts, Edit Contacts
It is used to access the Contacts on your phone to obtain the recipient's contact information (alias), which is then translated into the recipient's 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.

Notifications
The mobile application needs access to notifications for sending and receiving push notifications.

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.

Biometric identification, such as fingerprint and facial recognition, can be used instead of a password to log in to the Flik Pay mobile application and to confirm payment transactions in the Flik Pay mobile application. Fingerprint or facial data are stored exclusively on your mobile device. We do not process fingerprint and facial image data (we do not store or access these data), which means that we are not the controller of such personal data. Nor can it be considered that such data are processed by our contractual processor on our behalf. In view of the above, we do not guarantee the compliance of the processing of such personal data with ZVOP-1 or the GDPR. Moreover, we are not liable nor do we guarantee the security of the fingerprint identification and facial recognition function on any device and the operation of the function as provided by the device manufacturer.

The mobile application will ask for your consent to process the data necessary for additional features provided by the mobile application – optional permissions.

3. For what purposes do 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 data for payment with digitalized card to merchant through NFC communication (if the mobile device so allows);
- 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 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 if you have defined at least one contact (alias) in the Flik Directory;
- Receiving requests for payment if you have defined at least one contact (alias) in the Flik Directory;
- Viewing the status of transactions performed with the mobile application;
- Providing and monitoring your payment transactions;

- Receiving push notifications regarding important updates to the mobile application or other information related to the use of the mobile application;
- Enforcing our legal rights.

Based on the ZPPDFT-2 and the ZPlaSSIED, your data is also processed for the following purposes:
- identifying and verifying your identity;
- verifying the compliance of transactions with the intended purpose of business; record keeping and data retention.

Based on legitimate interests pursued by controllers and which are not overridden by your interests or your fundamental rights and freedoms, your data are also processed for the purpose of providing a better and safer user experience and functioning of the application, and to prevent possible fraud and scam.

With your consent, your data are processed for the purpose of using additional functionalities of the mobile application, as stated in item 2 under the optional permissions for the use of the mobile application.

4. Data retention

In accordance with ZPPDFT-2, data on executed transactions are kept for 10 years after the transaction or after the termination of the business relationship with you, according to legislation.

5. With whom we share the data

We do not provide or disclose data to third parties, unless we are required to do so by the law or other appropriate legal basis.

The processing of payment transactions on our behalf is performed by Bankart d.o.o., which has its registered office and registered address at Celovška cesta 150, 1000 Ljubljana and with which we have concluded an appropriate data processing contract and which is our contractual partner for the processing of personal data. Some parts of the above described personal data processing are carried out by a US-based sub-processor contracted by Bankart under Article 28 of the GDPR, and transfer of personal data to the EU is carried out based on standard contractual clauses (Commission Implementing Decision (EU) 2021/914 of 4 June 2021).

6. Push notifications and Opt-Out

We may occasionally send you push notification for important mobile application udpates or other information regarding the use of the mobile application. 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.

7. 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.

8. Automated decision-making

On the basis of the provisions of Articles 13 and 22 of the General Data Protection Regulation, we hereby inform you that the Bank uses automated decision-making when processing data on the use of Flik Pay only in the framework of anti-fraud procedures, pursuant to Article 22 (2)(a), as this processing is necessary for the implementation of legal obligations. Special categories of personal data are not processed. If you disagree with the result of the automated decision of the payment fraud prevention system, you can challenge this decision by stating your position and requesting the Bank to have the decision reviewed by its employee.

9. Right of access by the data subject

Under the GDPR you have a series of rights related to personal data processing, regulated in Articles from 15 to 22 of the GDPR.

Right to withdraw consent

If you have given consent to the processing of your personal data for one or more specific purposes as the data subject, you have the right to withdrawal your consent at any time. Immediately after receiving the withdrawal of your consent for one or more specific purposes, the Data Controller shall stop processing your personal data for the specific purpose. The withdrawal of consent for personal data processing shall not affect the lawfulness of processing of personal data based on consent before its withdrawal and the use of these personal data for legally or contractually specified purposes.

Right of access by the data subject to processed personal data

You have the right to obtain from the Data Controller confirmation as to whether or not personal data concerning you are being processed, and, where that is the case, access to the personal data and the following information: the purposes of the processing, the categories of personal data concerned, the recipients to whom the personal data have been or will be disclosed, the envisaged period for which the personal data will be stored, the source of personal data.

Right to have your personal data that are inaccurate rectified

You have the right to request that the Data Controller rectifies or completes inaccurate or incomplete personal data concerning you. The Data Controller will immediately notify you of the correction of your personal data.

Right to restriction of processing of personal data

You have the right to request that the Data Controller restricts processing of your personal data if such data are inaccurate, unlawful, no longer needed for the purposes of the processing or if objection has been made.

Right to deletition of personal data ("right to be forgotten")

You have the right to request the Data Controller to delete, without undue delay, your personal data that it has been processing, whereby the data that the Data Controller processes on the basis of the provisions of the law will only be deleted after the expiration of the period specified by the law. If personal data are erased at your request, you will be notified by the Data Controller of deletition.

Right to objection

In addition to the right to withdraw consent, if your personal data are used for information purposes and/or direct marketing, you can request in writing that your data stop being used for that purpose

at any time. If you object to processing for marketing purposes, the Data Controller will immediately stop processing personal data for marketing and information purposes.

Right to data portability

You have the right to have your personal data that are processed by the Data Controller transmitted directly from the Data Controller to another controller, where technically feasible. You can exercise the rights referred to in this item by sending a request by any means to your Data Controller (contact details are given in paragraph two of this Privacy Policy) or the contractual processor – Bankart d.o.o., Ljubljana, with registered office at Celovška 150, 1000 Ljubljana, telephone: +386 (0)1 583 41 00, e-mail: info@bankart.si. The request will be decided in 30 days of receipt, except in exceptional cases.

Right to lodge a complaint with a supervisory authority

If you consider that your rights have been infringed by data processing, you may file a complaint with the Information Commissioner at Dunajska cesta 22, 1000 Ljubljana.

10. 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.delavskahranilnica.si.

Ljubljana, 30th January 2024