MonduCard – Terms for the Use of Digital Cards

V 1.0.0

These Terms for the Use of Digital Cards ("Digital Card Terms") govern the use of the MonduCard as a digital card in digital wallet applications offered and operated by independent third-party providers ("Digital Wallets") ("Digital Wallets"). They supplement the MonduCard General Terms and Conditions ("MonduCard GTCs"). In case of conflict, the MonduCard GTCs prevail.

The Business Customer is responsible for ensuring that each Cardholder reads, understands, and complies with these Digital Card Terms.

1. Scope of Service

1.1. Cardholders may add their MonduCard to supported Digital Wallets listed in Annex 1. Through these Digital Wallets, Cardholders may initiate contactless payments at participating merchants and automated checkout terminals.

1.2. Online or in-app use of the MonduCard is permitted where the Digital Wallet provider supports such functionality and merchants accept it. This may require a separate agreement between the Cardholder and the provider of the Digital Wallet.

1.3. Mondu is not responsible for the availability, functionality, or security of Digital Wallets, devices, or third-party applications.

2. Permitted Applications and Devices

2.1. Only the Digital Wallets listed in Annex 1 are supported. Wallet apps may only be downloaded from official sources listed in Annex 2.

2.2. Cardholders must use a compatible device capable of processing NFC (Near Field Communication) transactions and supporting the relevant Digital Wallet.

2.3. Digital Wallet providers determine device and operating system compatibility. Insecure, outdated, modified, or otherwise unsupported devices may be blocked.

3. Data Processing

3.1. When the MonduCard is provisioned or used in a Digital Wallet, the following data may be processed:

- device information,
- tokenised card credentials,
- transaction data (amount, merchant, location, timestamp),

- authentication and authorisation data,
- wallet provider identifiers.

3.2. Data is processed for:

- provisioning of the ManduCard,
- tokenisation and secure credential management,
- transaction processing and authorisation,
- fraud prevention and security monitoring.

3.3. Wallet providers process data under their own privacy policies and may process data outside the EU/EEA. Mondu is not responsible for such processing.

3.4. Technical data may be deleted by wallet providers after authorisation in accordance with their retention rules.

4. Authorisation of Card Payments

4.1. A payment via a Digital Wallet is authorised when the Cardholder:

- unlocks the device using a device-specific authentication method (PIN, passcode, or biometric), and
- initiates payment in the Digital Wallet or holds the device near a supported terminal.

4.2. Device unlock mechanisms include the entry of a PIN, passcode, or the use of a biometric feature uniquely associated with the Cardholder. Biometric features may include, for example, fingerprint authentication via fingerprint sensor or iris or facial recognition via the device's camera.

4.3. For certain low-value contactless transactions, unlocking the device may not be required if permitted under applicable limits set by Mondu or Visa. The amount and usage limits set by Mondu apply.

4.4. For online or in-app transactions, authorisation occurs through the Digital Wallet on the registered device.

4.5. Once authorised, a payment order cannot be revoked.

5. Use of the Card

5.1. The Cardholder must, in addition to the security obligations defined in the ManduCard GTCs:

- enable device locking mechanisms,
- ensure no third party can unlock the device,
- store only their own biometric identifiers on the device,
- keep the digital card secured and download wallet apps only from permitted sources (Annex 2),
- promptly install device operating system updates,
- ensure that the digital device used for the Digital Wallet is stored securely and that no third party has access to the digital payment function,

- report suspected unauthorised access immediately.

5.2. If the device is lost, stolen, or compromised, the Cardholder must immediately block the ManduCard or remove it from all Digital Wallets.

5.3. Before transferring the device to any third party, the Cardholder must remove all digital card data and reset the device to factory settings if necessary.

6. Spending Limit

6.1. The ManduCard may be blocked via Mondu's designated blocking channels.

6.2. Wallet providers may offer additional options:

- blocking or removing the digital card for a specific Digital Wallet,
- blocking or removing the digital card for a specific device,
- disabling wallet-based payments via the provider's online interface.

7. Termination of the ManduCard Agreement

7.1. When the ManduCard Agreement ends, the digital version of the ManduCard cannot be used in any Digital Wallet.

7.2. Removing or blocking the digital card in a Digital Wallet does not constitute termination of the ManduCard Agreement.

8. Notification of Changes

8.1. 8.1 Mondu may notify Business Customers or Cardholders of changes to these Terms through the used Digital Wallet applications.

Annex 1 – Supported Digital Wallets

Google Wallet / Google Pay (Google Ireland Limited)

Annex 2 – Permitted Download Sources

Apple App Store

Google Play Store