

*SPECIAL TERMS AND CONDITIONS OF THE DIGITAL
CARD SERVICE*



Table of contents

INTRODUCTION	3
I. DEFINITIONS.....	3
II. DIGITAL CARD SERVICE.....	4
III. REGISTERING THE DIGITAL CARD	4
IV. DESCRIPTION AND USE OF THE DIGITAL CARD SERVICE	5
V. BLOCKING OF THE DIGITAL CARD.....	5
VI. OBLIGATIONS OF THE CARDHOLDER.....	6
VII. (NON-)EXECUTION OF TRANSACTIONS AND FRAUD PREVENTION.....	7
VIII. OBLIGATIONS AND LIABILITIES OF THE ACCOUNTHOLDER.....	7
IX. OBLIGATIONS OF THE BANK.....	8
X. PROCESSING OF PERSONAL DATA AND DATA SHARING.....	9
XI. AMENDMENTS TO THE DIGITAL CARD SERVICE SPECIAL TERMS AND CONDITIONS.....	9

INTRODUCTION

In addition to the General Terms and Conditions and the Debit Card Special Terms and Conditions, these special terms and conditions (the **Digital Card Service Special Terms and Conditions**) govern the specific rights, obligations and responsibilities arising from the use of the Digital Card Service, both for the holder of the Digital Card and the holder(s) of the Account(s) to which the Digital Card is linked, as well as the Bank.

In case of contradiction with the General Terms and Conditions and the Debit Card Special Terms and Conditions, the Digital Card Service Special Terms and Conditions prevail over the other terms and conditions. All terms and conditions are always available free of charge in French, Dutch and English at www.medirect.be.

I. DEFINITIONS

Authentication Method	A personalised identification method needed to unlock the Cardholder's Electronic Device, such as a number code, pattern, fingerprint or face scan. This is a personalised security feature that the Cardholder may be required to use to sign certain Transactions, depending on the Digital Card Services Provider and the Electronic Device used by the Cardholder.
Digital Card	A digitalised version of the Physical or Virtual Card, linked with a Digital Card Service offered by a Digital Card Services Provider..
Digital Card Service	A Service provided by a Digital Card Services Provider, whereby the Cardholder can use a Digital Wallet allowing him to store his Digital Card on his Electronic Device for contactless payments, in-app purchases and other electronic payments, such as Apple Pay, Google Pay and any other similar Service that the Bank may add in the future.
Digital Card Services Provider	The entity providing Digital Card Services via the Cardholder's Electronic Device.
Digital Wallet	An application managed by a Digital Card Services Provider on an Electronic Device, that stores payment details of the Client saved therein, including details related to the debit Card, and uses authentication and data encryption to protect the Client's personal information.
Electronic Device	An electronic instrument supporting Payment Transactions that use a Digital Card Service and meets the Digital Card Services Provider's technical requirements and allows the Cardholder to access the Digital Card Service. This



may be a smartphone or smartwatch equipped or not with NFC technology, a laptop, etc.

NFC

Near Field Communication, a technology that allows contactless payments by bringing an Electronic Device containing a Digital Card linked to a Digital Card Service near to an NFC-equipped terminal.

II. DIGITAL CARD SERVICE

(§ 1) The Digital Card Service is available to Cardholders for the purposes of purchasing goods and services using contactless payments with an Electronic Device at payment terminals equipped with NFC technology and via on-line merchants (in app or through website) who accept these as a mode of payment.

(§ 2) Digital Card Services Providers may establish their own terms and conditions, to which the Cardholder may be requested to accept. These terms and conditions are not binding on the Bank. The Cardholder is responsible for confirming that their Electronic Device meets the Digital Card Service Provider's technical requirements and allows the Cardholder to access the Digital Card Service. The Bank declines responsibility for technical errors, interruptions and defects in the services provided by Digital Card Services Providers. The Bank also declines liability for the consequences of changes made by a Digital Card Services Provider to a Digital Card Service, including discontinuation of the service).

III. REGISTERING THE DIGITAL CARD

(§ 1) In order to use the Digital Card Service, the Cardholder must register his Digital Card as required by the Digital Card Services Provider. To this end, the Cardholder can initiate the process on his Electronic Device either via the Banking app or via the Digital Wallet provided by the Digital Card Services Provider and must follow the instructions either in the Banking app or in the Digital Wallet. He will be requested to accept the applicable terms and conditions of the Digital Card Services Provider and the current Digital Card Service Special Terms and Conditions. The Cardholder will be required to enter his personal details and Card details in the Digital Card Service.

(§ 2) The Cardholder understands that the use of a rooted or jailbroken Electronic Device in relation to the Digital Card Service is expressly prohibited and constitutes a violation of the Digital Card Service Special Terms and Conditions and is grounds for the Bank to deny use of the Digital Card.

(§ 3) By adding his Digital Card to the Digital Card Service, the Cardholder understands that a unique identifier (different from his Card number) will be allocated for the purpose of making purchases and receiving refunds through the Digital Card Service.

(§ 4) The Digital Card Services Provider may limit the number of Digital Cards that the Client may store on one Electronic Device.

(§ 5) If the Cardholder no longer wants to use his Digital Card, he must follow the instructions from the Digital Card Services Provider to remove the Digital Card from his Digital Wallet. Removing the Digital Card from the Digital Card Service will not terminate the Card, unless the Cardholder also chooses to terminate his Card in accordance with the Debit Card Special Terms and Conditions.

IV. DESCRIPTION AND USE OF THE DIGITAL CARD SERVICE

(§ 1) The Cardholder can make payments with his Digital Card using the Digital Card Service to carry out Payment Transactions, under the terms and conditions laid down by the Digital Card Services Provider, the Debit Card Special Terms and Conditions and the Digital Card Service Special Terms and Conditions.

(§ 2) The Cardholder consents to a Payment Transaction by using his Electronic Device's means of access and signature, as follows:

- contactless payments in physical stores: by holding his Electronic Device against the NFC-equipped payment terminal. Depending on the Digital Card Services Provider and the Payment Transaction amount, the Cardholder may be prompted to use his Authentication Method;
- in-app purchases and other electronic payments: by choosing the Digital Card Service from the payment options offered and then giving permission by using his Authentication Method when prompted.

When using the Digital Card Service as described, the Cardholder is deemed to consent to all Transactions taking place via the Digital Card Service. The Accountholder irrevocably authorises the Bank to debit the Account for the amount of the Payment Transaction submitted via the Digital Card Service. The Cardholder and the Accountholder admit the legally binding nature of Transactions carried out using the Digital Card Service as described. Payment Transactions executed as such constitute valid and sufficient evidence of their agreement with the existence and content of the Payment Transaction.

(§ 3) The Bank reserves the right to refuse to execute a Payment Transaction and will inform the Cardholder as soon as possible, and, if possible, tell the reasons for this refusal. This notification will be given via the merchant's payment terminal, webshop or app.

(§ 4) Some Digital Card Services Providers offer Cardholders a history of the most recent payments made using the relevant Digital Card Service, based on information provided by the Bank.

V. BLOCKING OF THE DIGITAL CARD

(§ 1) The Bank reserves the right to block the use of the Digital Card within the Digital Card Service for objectively justified reasons relating to the security of the Digital Card (or the underlying Card) or where there is a suspicion, of unauthorised or deceptive use of the Digital Card (or the underlying Card), e.g. if the Bank believes that the Electronic Device may have been used fraudulently or without authority in a Digital Card Service.

(§ 2) The Cardholder will be notified of this measure by the Bank, prior to the blocking where possible, or immediately hereafter, unless the provision of this information is impeded for objectively justified security reasons or prohibited by applicable law.

(§ 3) Once the reasons justifying the blocking no longer exist, the Bank will unblock the Digital Card.

VI. OBLIGATIONS OF THE CARDHOLDER

(§ 1) Next to the general obligations of the Cardholder contained in the Debit Card Special Terms and Conditions, the Cardholder

- will not store his Authentication Method (e.g. if a PIN is used) and Electronic Device together or write the Authentication Method, in any form whatsoever or disclose it orally (e.g. if a PIN is used);
- will not give access to his Electronic Device to third parties (including his partner, family and friends);
- will not leave his Electronic Device unattended in any place effectively open to the public or in a vehicle – even if it is locked;
- will immediately report the loss, theft or unauthorised use of his Electronic Device;
- will immediately request the Bank (phone number +32 (0)2 887 20 05) (or any third party handling these requests on behalf of the Bank) to block his Card upon realising that his Electronic Device was lost, stolen or misused or realising that the safety of his Electronic Device or Authentication Method is compromised;
- will remove a Digital Card from an old Electronic Device which is no longer in personal use;
- will use at all times the most recent version of the Digital Card Services Provider's software and an Electronic Device that complies with its security and system requirements.

(§ 2) The Bank declines responsibility for:

- all and any prejudice (direct or consequential) attributable to operations of a Cardholder's Electronic Device or third-party telecommunications services or an interruption in services as the result of circumstances beyond its control;
- damage or modification to a Cardholder's Electronic Device as a result of installing, upgrading, updating or using the Digital Card Service;
- temporary unavailability, suspension, interruption or slowness of the Digital Card Service due to maintenance, defects of force majeure and any other cause that cannot otherwise be reasonably construed as within the Bank's control;
- prejudice of any kind resulting from difficulty in, or the impossibility of, downloading or accessing the Digital Card Service or accessing content of the Digital Card Service or another fault in telecommunications systems causing the unavailability of the Digital Card Service;
- prejudice due to the unavailability of third-party websites or information linked to within the Digital Card Service or as a result of the falsity, incompleteness or inaccuracy of information, whereby no such third-party information will imply obligations due by the Bank;

- direct or consequential prejudice resulting from or in relation to (defective) operation of a Cardholder's Electronic Device or third-party telecommunications services, software or hardware, such as the Digital Card Services Provider.

VII. (NON-)EXECUTION OF TRANSACTIONS AND FRAUD PREVENTION

(§ 1) The Bank reserves the right to freeze the Client's card(s), or to refuse to process, in whole or in part, his transactions if required by law, a court decision or by the supervisory authority, or any other objective reason, particularly in the event of suspected use of the Bank's Services to execute or facilitate fraudulent or illegal operations, for example relating to suspected money laundering.

(§ 2) The Bank reserves the right to systematically deny any and all transactions to counterparties identified by the Bank as likely to facilitate fraudulent or illegal activities.

(§ 3) The Bank shall not be held liable for processing a transaction that it is not obliged to process by virtue of the present article. In particular, if the balance of the Client's Account is not sufficient to cover the amount of the transaction, increased with the costs, and fees or expenses incurred, the Client shall pay the negative balance of his Account and the Bank may exercise all its rights in this respect, in particular its right of set-off against other Accounts of the Client.

VIII. OBLIGATIONS AND LIABILITIES OF THE ACCOUNTHOLDER

(§ 1) When an Accountholder notices, on his Account statements, a Payment Transaction that is either unauthorised (a Payment Transaction is deemed authorised if the client gave his prior consent to the Operation as described in article IV.§2) or incorrectly executed, as well as any error or irregularity on his Account, he must immediately notify the Bank at the latest within thirteen months following the value date of the debit. In the event of an unauthorised Payment Transaction, the Bank will immediately refund the Accountholder, except when there is a presumption of fraud or gross negligence in the hands of the Cardholder, or if the Cardholder has not complied with his obligations in article VI.

(§ 2) Where applicable, the Account that was debited will be restored as if the unauthorised or incorrectly executed Payment Transaction had not taken place. Any other incurred charges or fees will also be refunded. The Bank bears the burden of proof that the Payment Transaction was duly authenticated, recorded and accounted for and that it was not carried out as a result of a technical defect or any other problem.

(§ 3) The Accountholder shall bear the losses of any unauthorised Payment Transaction resulting from the stolen or misappropriated Electronic Device up to a maximum of 50 euros, up until the moment he or the Cardholder (if these are separate individuals, to be pre-approved in writing by the Bank on a case-by-case basis) has notified the Bank in accordance with article VI. However, if these losses result from the Cardholder's or the Accountholder's (if these are separate individuals, to be pre-approved in writing by the Bank on a case-by-case basis) intentional or grossly negligent failure to comply with one or more of their obligations under the Debit Card Special Terms and

Conditions and the Digital Card Service Special Terms and Conditions, the Accountholder shall bear all losses caused by unauthorised Payment Transactions (in this case, the limit of 50 euros shall not apply) up until the moment he or the Cardholder has notified the Bank in accordance with article VI.

(§ 4) If the Cardholder acted fraudulently or with gross negligence, the Accountholder shall bear all losses resulting from an unauthorised Payment Transaction carried out both before and after the notification referred to in article VI (notwithstanding the Bank's obligation to take all necessary measures to prevent the use of the Digital Card).

(§ 5) Gross negligence includes among others, but not limited to:

- the Cardholder writing his personal security details (e.g. Authentication Method) in an easily recognisable form and particularly on an object or document kept or carried by the Cardholder with his Electronic Device;
- the Cardholder not notifying the Bank of the loss or theft of his Electronic Device as soon as he became aware of it.

Depending on circumstances, other incidents could also qualify as gross negligence irrespective of whether they result from the Cardholder not complying with his obligations under the Debit Card Special Terms and Conditions or under the Digital Card Service Special Terms and Conditions.

(§ 6) As an exception to the above rules, the Accountholder shall not bear any losses in the following cases, unless the Cardholder/Accountholder acted fraudulently or with gross negligence:

- the loss, theft or misappropriation of the Electronic Device could not be detected by the Cardholder prior to the Payment Transaction;
- the loss is due to acts or omissions of an employee of the Bank or of a subcontractor;
- when the Payment Transaction did not require the use of a strong user authentication (in particular the use of an Authentication Method), unless the Cardholder/Accountholder acted fraudulently.

IX. OBLIGATIONS OF THE BANK

The Bank must meet the following obligations:

- it must ensure that the personal security details of the Digital Card (and the underlying Card) do not become accessible to parties other than the Cardholder authorised to use the Digital Card;
- it must make sure that the Cardholder can always make the notifications described in article VI, by providing the appropriate means to do so;
- It must ensure that the Cardholder can ask for the blocked Card to be released, which the Bank will effectively do so after having checked that all the conditions to unblock are met;
- it must be able to provide the Cardholder, if he requests so and for 18 months as from the notification described in article VI, proof of the given notification;
- it must prevent the Digital Card from being used once the notification described in article VI has been given;

- it maintains internal Transactions registers for a period of at least 10 years from the time the Transactions were carried out.

X. PROCESSING OF PERSONAL DATA AND DATA SHARING

(§ 1) The Bank and the Digital Card Services Provider collect and process personal data from the Cardholder when he enters his Digital Card in a Digital Card Service. The Bank does so in accordance with its Privacy policy (available on its website www.medirect.be). The Bank and the Digital Card Services Provider each act as separate controllers:

- the Digital Card Services Provider is the controller of the personal data relative to the Digital Card Service and its functionalities (which the Bank is not involved into);
- the Bank is the controller for transactions done using the Digital Card.

(§ 2) The Bank processes personal data amongst others for verification and proper execution of Payment Transactions made with the Digital Card using the Digital Card Service. In this connection, the Bank processes the specific technical details of the transaction, such as the Card number, amount and Payee's name. In addition, the Bank also receives logs of the technical features of the Electronic Device on which the Cardholder uses the Digital Card Service, such as the name of the Electronic Device, relevant identifiers of the Electronic Device, the IP address and the name of the telecom operator (if applicable).

(§ 3) The Bank exchanges details concerning the Cardholder, the Accountholder and Payment Transactions performed via the Digital Card Service with the Digital Card Services Provider. The Digital Card Services Provider uses this information to detect and combat fraud, to analyse and improve use of the activities of the Digital Card Service and promotions for the Digital Card Service. The Digital Card Services Provider may report to third parties on numbers of service users. The Digital Card Services Provider may also pass personal data to third parties where required by law and where third parties process information on behalf of the Digital Card Services Provider. Where the personal data for the Digital Card Service is processed by the Digital Card Services Provider outside the European Union, it has bound itself not to do so other than in accordance with European data protection rules. Data processing by the Digital Card Services Provider falls outside the Bank's responsibility. Details of how personal data is processed by the Digital Card Services Provider are available to Cardholders in the relevant Digital Card Service's privacy documentation.

(§ 4) The Bank processes personal data in a lawful, fair and transparent manner. Details of how the bank process and shares Cardholder's personal data are available to them in the Bank's privacy statement, which includes information on their rights and how to exercise them. The privacy statement is available on the website of the Bank (www.medirect.be) and is subject to regular updates.

XI. AMENDMENTS TO THE DIGITAL CARD SERVICE SPECIAL TERMS AND CONDITIONS



(§ 1) The Bank may amend or complete at its own discretion the Digital Card Service Special Terms and Conditions by sending a Notification to the Client. Such changes will come into force on a date to be specified in the Notification and the effective date will be at least two (2) months after the date on which the Notification is sent, unless the change(s) is/are technical, editorial or formal, is/are required by or related to an update of the law or regulation or do not prejudice the rights of the Client, in which case the effective date may be earlier.

(§ 2) If the Client does not inform the Bank that he does not accept the amendments to the Digital Card Service Special Terms and Conditions before they come into force, he shall be deemed to have accepted them. Clients who do not accept the new Digital Card Service Special Terms and Conditions before they come into force may terminate the Digital Card Service linked to the Card immediately and without charge.