



Privacy Policy: itsme APP

This privacy policy applies to the itsme Application (hereafter the itsme App or the App) developed by Belgian Mobile ID SA/NV (the Privacy Policy).

The itsme App (the App) allows its users (hereafter the Users) to register with, access/log-into and approve transactions through websites and/or different mobile applications (as made available by Service Providers). At a future date the App and its services could be extended to cover qualified electronic signature services (hereafter all services together -actual and future- the Mobile ID Services).

The App is made available by Belgian Mobile ID NV/SA, whose seat is registered at Sint-Goedeleplein 5, 1000 Brussels, Belgium, under number 0541.659.084 (hereafter Belgian Mobile ID, we or us).¹

The Mobile ID Services are made available by Belgian Mobile ID with the intervention of several third parties (the Belgian Mobile ID Members):

- Service Providers: providers of services or goods or any other third party with whom you use the App to register with them, or log into their website/app or approve a transaction.
- SIM Controllers: your telecommunications operator.
- Identity Registrars: entities that can verify your identity, such as your bank.

Belgian Mobile ID acts as data 'controller' under the applicable Belgian privacy laws, and as such Belgian Mobile ID is responsible for the collection and use of your personal data.

The following policy explains the different elements of personal data that will be collected, the purposes of collection, any sharing of that data with third parties, your rights as the data subject and the measures taken to protect your personal data. Please note that the Mobile ID Services necessarily imply that we will collect and store personal data pertaining to you and that we will communicate some elements of your personal data to third parties, as described below.

This Privacy Policy only describes the processing of personal data performed by us or on our behalf in the context of the Mobile ID Services – the SIM Controllers, Service Providers and Identity Registrars also process your personal data as data controllers in the context of their own services or activities; for those processing activities please refer to their privacy policies.

¹ The Crossroads Database of Undertakings (Banque-Carrefour des Entreprises/Kruispuntbank van Ondernemingen).



1. THE PERSONAL DATA WE COLLECT AND HOW

1.1. The Personal Data we process

In order to offer the Mobile ID Services and operate the App as set out in this Privacy Policy and the General Terms and Conditions, we process different categories of personal data:

- **Identity data**, which allows us to identify you. These cover various kinds of data:
 - core identity data, consisting of your full name, gender, legal address, nationality, date and place of birth, ID number and e-ID picture (all as recorded on your e-ID card);
 - National register number, which will only be used in the context of your use of Mobile ID Services with applications or websites offered by public services (Tax-on-web, for example) and within strict legal limits
 - Contact information (email address and mobile phone number);
 - Different user and preference settings, e.g. your shipping address or the specific capacity in which you act (as employee of a specific company, for instance).

- **Security data**, which are necessary in order to verify your identity as the User and to link your phone to your account, i.e. details regarding your device (brand, version, rooted or not device, ...), your device's operating system (OS and version), the version of the itsme App on your device, the status of your subscription with your mobile operator and the country in which you are (including but not limited to the device identifier ("IMEI"), the SIM card ("IMSI" or "ICCID"), the code of your mobile network operator (identifying your mobile network operator, "MNC") and the mobile country code (identifying the country in which you are, "MCC"). When you enrolled for the Mobile ID Services, you consented to the transfer of some of the security data by the SIM Controller to Belgian Mobile ID; the other elements of the security data are collected directly via your device. .

- **Operation data**, which are the records of specific operations carried out through the App and their characteristics, covering for example, to which entity information is sent, when it is sent and concerning which transactions.

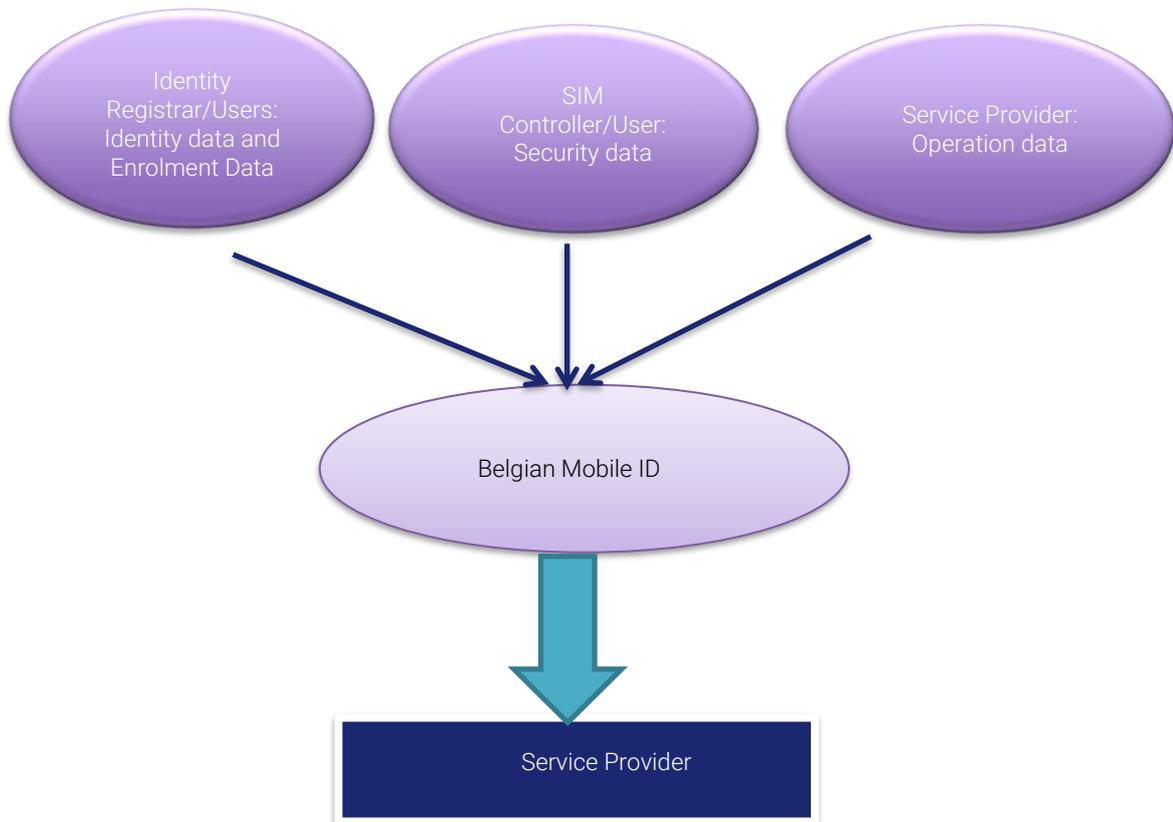
- **Enrolment data**, which are specifics regarding the registration process and cover information such as your consent to our terms and conditions and privacy policy and the date and time of enrolment.

All the data mentioned above are mandatory in order to benefit from the App's functions and Mobile ID Service. We could process other data elements on a voluntary basis, but in such case we would inform you and ask for your consent thereto.

Concerning the national register number

The national register number is only necessary (and will only be processed) in order to allow you to access, through the Mobile ID Services, to some websites or applications offered or managed by public services (e-Health, Tax-on-web, for example). If you do not want to use Mobile ID Services to access to websites or applications offered or managed by public services, please let us know through our email address : privacy@itsme.be

1.2. How Personal Data Are Collected



The different categories of personal data described are either collected directly from you or by a Belgian Mobile ID Member as follows:

- **Identity data** is collected either directly from you or from the Identity Registrar you enrolled with for the App. When you enrolled with them you consented to the transfer of your identity data to Belgian Mobile ID.
- **Security data** is obtained either directly from your phone (the location data, i.e. the country in which you are ('MCC') and your telecom operator (MNC)) or from the SIM Controllers (details regarding your device (IMEI) and your SIM card (IMSI)).
- **Operation data** is a mixture of data generated by the App itself and data received from Service Providers.
- **Enrolment data** is created when registering for an itsme account. Enrolment Data is obtained either directly from you, when registering through the itsme website, or through the Identity Registrar.

2. WHAT IS THE PERSONAL DATA USED FOR?

The personal data we collect are used to provide you with the Mobile ID Services, it being understood that this includes:

- carrying out the operations you request to perform with the App and more generally, the operation of the App and performance and Mobile ID Services;
- the operation, evaluation and improvement of the services offered by Belgian Mobile ID, such as: (i) managing our communications with you, (ii) monitoring the usage of the Mobile ID App after a publicity or marketing campaign, (iii) analyzing Belgian Mobile ID's products, services and websites, (iv) facilitating the functionality of the App and (v) performing accounting, auditing, billing, reconciliation and collection activities;



- fraud management and risk management; and
- any processing required for compliance with applicable legal requirements and industry standards and policies applicable to Belgian Mobile ID.

The different categories of personal data are processed for the purposes and in the manner as described below.

2.1. When Will Identity Data Be Processed and How:

- **Registering for the Mobile ID Services:** we will collect your identity data the first time you register for the Mobile ID Services (either via an Identity Registrar or directly from you) after you consented thereto.
- **Registration with a Service Provider:** Every time you register for the first time with a Service Provider through the App, your consent is requested. This is because in such case we will have to transfer elements of your identity data to them. You will be asked to consent to each data transfer and to any additional data request should it arise.
- **Logging-in and Approving a Transaction:** Depending on the technical interface Service Providers choose, identity data may have to be communicated to them for log-in and approval operations.
- **Archiving:** Once you have terminated your use of the Mobile ID Services or after a period of inactivity over two years, the data will be archived for evidentiary purposes for a period of 10 years (counting from the last transaction), after which they will be destroyed.

All elements of your identity data that are communicated to Service Providers will be processed by those Service Providers acting as data controllers in accordance with their own privacy policy – please note that once elements of identity data are transferred to the Service Providers we cannot control how they will process them nor do we assume any liability therefore. We advise you to read carefully the Service Providers' privacy policy before using our App to perform operations with them.

Processing of your fingerprint data: the digital fingerprint(s) that you register on your device, will not be transferred to BMID in whatever form, where you have activated the function for digital fingerprint recognition in your profile and use such a function on the device that you use for the Mobile ID Services. These fingerprint data are not processed by BMID. The Mobile ID Services only consult the fingerprint recognition function on your device and only receives confirmation data that the fingerprint used by you corresponds to the fingerprint that has been logged by the device. The processing of the User's personal data in the context of the function for digital fingerprint recognition is subject to the privacy policy and terms and conditions of the manufacturer of the device.

2.2. When Will Security Data Be Processed and How:

- **A transaction requires identity verification:** we will receive the security data partly from the SIM Controllers (IMSI and IMEI at the time of enrolment and in specific cases at the moment of an operation transaction with the App) and partly directly from your phone (data regarding your location and IMSI and IMEI for each transaction with the App). We will store that information in our database as long as needed to be able to compare those data to those received from your phone in order to ensure that they are consistent. In certain limited cases, elements of the security data will be transferred to a Service Provider for purposes of fraud and risk management by that Service Provider. You will be notified through the App of any such transfers before they occur.
- **Archiving:** Once you have terminated your use of the Mobile ID Services or after a period inactivity over two years, the security data will be archived for evidentiary purposes for a period of 10 years (in case of transaction data, counting from the last transaction), after which they will be destroyed.

All elements of your security data that are communicated to Service Providers will be processed by those Service Providers acting as data controllers in accordance with their own privacy policy – please note that once elements of security data are transferred to the Service Providers we cannot control how they will process them nor do we assume any liability therefore. We advise you to read carefully the Service Providers' privacy policy before using our App to perform transactions with them.

2.3. When Will Operation Data Be Processed and How:

- **Carrying out a transaction:** the App generates the operation data as you carry out different operations with Service Providers. The data generated will be logged for evidentiary purposes.



- **Archiving:** the operation data will be archived for evidentiary purposes, for a period of 10 years (to be calculated starting from the relevant operation), after which they will be destroyed.

2.4. When Will Enrolment Data Be Processed and How:

- **At the enrolment:** the enrolment data will be generated and collected at the time of your enrolment with the Mobile ID Services;
- **Evidence and Archiving:** enrolment data is kept in database by either the Identity Registrar (acting as processor for Belgian Mobile ID) or directly Belgian Mobile ID for evidentiary purposes. Once you have terminated your use of the Mobile ID Services or after a period of inactivity over two years, the data will be archived for a period of 10 years. After this period, the enrolment data will be destroyed.

Please also note that by contacting our facilities, including the helpdesk services linked to the itsme App, you agree that messages (voice, text or otherwise) and any related technical information (such as the origin of communication, time and duration of the communication, claimed identities of the participants) may be recorded and stored for one month, in order to permit us to evaluate the effectiveness and performance of our contact facilities, and in order to address any attempted unlawful uses of our contact facilities.

3. THE PERSONAL DATA WE SHARE

We do not sell or otherwise disclose personal data we collect about you to third parties, except as described in this Privacy Policy (here above and below). We will share personal data to enable the performance of Mobile ID Services that you have chosen to use. In this respect, we may share your personal data with our members, including Service Providers, as described above.

We transfer data to third parties who process data in the context of performing Mobile ID Services on our behalf (subcontractors). Those actors are not authorized to use the data or disclose it in any way except as here above described or to comply with legal requirements. We contractually require these third parties and our Members to appropriately safeguard the privacy and security of personal data they process on our behalf.

We also may disclose data about you: (i) if we are required to do so by law or legal process, (ii) to law enforcement authorities or other government officials in accordance with their competences, or (iii) when we believe disclosure is necessary or appropriate to prevent physical harm, or (iv) in connection with an investigation of suspected or actual fraudulent or illegal activity.

We also reserve the right to transfer any personal data we have about you in the event we sell or transfer all or a portion of our business or assets affecting the itsme App. Should such a sale or transfer occur, we will ensure that personal information you have provided to us remains to be treated in a manner that is consistent with this Privacy Policy.

4. YOUR RIGHTS AND CHOICES

4.1. Access, Rectification and Data Portability

At any time, you may exercise your right to access and rectify any of your personal data that we may retain in relation to the itsme App, in accordance with applicable data privacy laws, either, for some date, through the App interface itself, or by sending a request with a copy of the front of your ID card, passport or other proof of identity to privacy@itsme.be, or in writing to Belgian Mobile ID NV/SA, Data Protection Officer (DPO), Sint-Goedeleplein 5, 1000 Brussels, Belgium.

Please note that some elements of your personal data can be accessed through the App's interface and as the User you have the right to rectify and modify this data at any time. However, because the Mobile ID services' security depends on the integrity of the core identity data, the modification of these identity data will only be possible by following the steps of enrolment: either through an Identity Registrar or via the itsme website (both of which require additional steps to verify your identity).

Finally, as soon as applicable, you will also have the right to data portability in accordance with applicable data privacy laws.



4.2. Erasure

You may at any time exercise your right to data deletion in accordance with applicable data privacy laws, by sending a request with a copy of the front of your ID card, passport or other proof of identity to privacy@itsme.be, or in writing to Belgian Mobile ID NV/SA, Data Protection Officer (DPO), Sint-Goedeleplein 5, 1000 Brussels, Belgium. Belgian Mobile ID will refrain from using any of your personal data upon this request and will only continue to store any past personal data for evidentiary purposes over a period of ten years, after which they will be erased. After your data has been deleted, you will no longer be able to use the BMID services. As soon as Belgian Mobile ID has received the erasure request, it will inform all Service Providers to whom BMID has provided any of your identity data. Please note that this notification is for information of the Service Provider only and that the Service Provider will independently decide to continue using the data afterwards or not.

4.3. Objection

When using the itsme App you could be requested to consent to certain data processing activities. You have the right to withdraw your consent to such activities at any time, by sending a request with a copy of the front of your ID card, passport or other proof of identity to privacy@itsme.be, or in writing to Belgian Mobile ID NV/SA, Data Protection Officer (DPO), Sint-Goedeleplein 5, 1000 Brussels, Belgium. Such withdrawal will not affect the lawfulness of past data processing. Please note that opposing to some processing can, however, impact your continued use of the App as Belgian Mobile ID cannot provide the Mobile ID Services without processing necessary elements of your personal data.

At any point, should you deem that your rights have not been respected, You may also log a complaint with the Belgian Commission for the Protection of Privacy, rue de la Presse, 35, 1000 Brussels, e-mail address: commission@privacycommission.be (see also www.privacycommission.be).

5. HOW WE PROTECT PERSONAL DATA

We maintain appropriate administrative, technical and physical safeguards to protect personal data against accidental or unlawful destruction, accidental loss, unauthorized alteration, unauthorized disclosure or access, misuse, and any other unlawful form of processing of the personal data in our possession.

The security measures we adopt depend on the different types of information collected and stored.

5.1. How We Ensure the Integrity of Stored Data

– Encryption

We encrypt all the data we store with different keys depending on the origin of the data.

When you provide personal data online, we use the industry standard for encryption on the Internet – Secure Socket Layer (SSL) technology – to help protect the data that you provide. This internet encryption standard scrambles data as they are transferred from your device to our server. We also use digital certificates to ensure that you are connected to authentic channels.

– Data Storage

All of your personal data, whether used actively or archived, is stored in Belgian Mobile ID's servers and not the App itself. Belgian Mobile ID uses secured servers provided by a provider internationally certified ISO 27001 that are located in Belgium to store the data. No personal data will be stored outside of the European Union.

– Restricted Access

Internal access to the personal data is limited on a strict 'need-to-know' basis. Only authorized personnel, whose activity will be monitored to prevent any misuse, will be able to access the data.

5.2. Measures Preventing Misuse

Each operation will be subject to strict authentication mechanisms.



6. DATA TRANSFERS

We do not transfer any of your personal data outside of the European Economic Area, nor in any manner not specified here above.

7. UPDATES TO THIS PRIVACY POLICY

This Privacy Policy may be updated periodically to reflect changes in our personal data practices. We will post a prominent notice on our websites and/or through the itsme App to notify you of any significant changes to our Privacy Policy and indicate at the top of the notice when it was most recently updated. Where required, You will be asked to renew Your consent to this Privacy Policy.

8. HOW TO CONTACT US

If you have any questions or comments about this Privacy Policy, if you would like to exercise your rights, or to update the information we have about you or your preferences, please contact us here:

Belgian Mobile ID NV/SA
Sint-Goedeleplein 5
1000 Brussels
Belgium
Tel.: +32 (0) 2 657 32 13
Email: privacy@itsme.be