MY DIGITAL KEYS - TERMS OF USE

Article 1 – Scope of application of the present terms of use

The present terms of use regulate the procedure made available by the Federal Government for the electronic registration, identification and authentication of end users, who may or may not be citizens. Using this procedure enables end users to register with a view to gaining safe access to electronic services provided by the various Belgian authorities and safe electronic communications with the said authorities.

Nonetheless, it may be that some public bodies have different systems in place for electronic end user management.

Article 2 - Access to the procedure

The end user has access to the procedure, albeit without any guarantees being offered that access to the procedure and the services made available shall be guaranteed at all times or be free from errors or technical disruptions.
Access to the procedure may be disconnected at any point in time, in full or in part, (for maintenance purposes, in amongst other things). Insofar as reasonably possible, the end user shall be notified of such interruptions ahead of time.
The end user shall have access to certain services made available by the various Belgian authorities only upon completing the applicable registration, identification and authentication procedure.
In doing so, the end user shall be required to:
 agree to the present terms of use;
 provide a working e-mail address.

If necessary, the end user shall be required to amend the details relating to him/her to ensure they are up to date and accurate at all times.

Article 3 - Use of digital keys

The end user's access to specific services, which are made available electronically, requires the use of digital keys (eID card reader, wireless eID card reader, security code by mobile app/text message/token and username and password, …).
These digital keys and the details associated therewith are strictly personal and non-transferable.
Each end user is responsible for the safekeeping, protection, confidentiality and management of his/her digital keys and the details associated therewith.

The end user is responsible for choosing a safe password or other secret code.
If an end user is aware that his/her username, password, token or other digital key has been lost, or is being unlawfully used by third parties, or suspects such loss or unlawful use, he/she is to promptly put in place all relevant steps to deactivate the digital key as set out in article 6 and elsewhere.

In the event his/her digital key should be locked, the end user is to apply for a new digital key.

Article 4 - Use of the e-mail address
The end user is responsible for choosing the e-mail address communicated by him/her. He/she hereby confirms that the said e-mail address belongs to him/her and that no third parties are allowed to use the said e-mail address without his/her permission.

The end user hereby confirms the said address is used by him/her on a regular basis.

Article 5 - Use of the procedure
Each end user is duty-bound to:
1. provide comprehensive, accurate, truthful information that is not misleading;

2. to act in compliance with the provisions set out in the statutory laws, regulations, decrees, ordinances, and decisions adopted by the Federal, regional, local or international authorities;

3. to refrain from manipulating the information supplied in any way, shape or form, or using any which technologies.

Article 6 - Procedure in the event of loss or alteration of a digital key or part of a digital key

In the event the end user should lose his/her identity card or other identity document, the holder thereof is required to report this at his/her earliest convenience to the registry office of his/her town or the nearest police station, or to get in touch with the DocStop department of the Federal Public Service of Home Affairs.

In the event an end user should lose his/her smartphone or mobile phone, or have the said device stolen, he/she shall be required to report this to his/her service provider at his/her earliest convenience. In addition, he/she is to delete the keys in question under “My digital keys” (security code via mobile app and/or security code by text message).

In the event an end user wishes to use a new mobile phone number, he/she shall be required to first delete the “security code by text message” key for the old number under “My digital keys”.

In the event an end user should cancel his/her MYDIGIPASS account, he/she shall be required to delete the “wireless eID card reader” key under “My digital keys”.

In the event an end user should lose his/her token, he/she is to deactivate the said token. He/she is subsequently free to apply for a new token under ”My digital keys". In the event of a new application, the system will generate a new token which will be sent to the end user’s official address as recorded in the National Register by conventional post. The old token will be deactivated as soon as possible and will no longer be available to be used from that time forward.

Article 7 - Personal privacy protection

The Government is keen to protect your privacy and in doing so acts in compliance with the provisions of the Belgian Privacy Act *(Act of 8 December 1992 personal privacy protection in relation to the processing of personal details)*.

By performing the above registration procedure, the end user unreservedly and unambiguously gives his/her permission for his/her personal details to be used. He/she acknowledges that the processing of these personal details is pertinent and necessary to allow users to be accurately and safely identified and authenticated in order to enable secure user management and electronic communications to occur between the end user and the Government.

The end user hereby expressly consents for his/her National Register number to be stored in the system and acknowledges that keeping the said number on record is pertinent and necessary for the proper operational running of the system. To this end, Powered by FOD Beleid en Ondersteuning – DG Digitale Transformatie holds the relevant authorisations delivered by the Sectoral Committee of the National Register.

Some login details are consulted in the National Register or in the BIS register. To this end too, Powered by FOD Beleid en Ondersteuning – DG Digitale Transformatie holds the relevant authorisations.

Powered by FOD Beleid en Ondersteuning – DG Digitale Transformatie is responsible for the processing of these personal details and acts to make sure that the said details are protected and remain confidential. Powered by FOD Beleid en Ondersteuning – DG Digitale Transformatie is responsible for answering questions with regard to the protection of personal details. The personal details entered by the end user are transmitted over the Internet using the SSL protocol. The personal details are only made available to other public services that use the said protocol to identify and authenticate end users with a view to giving the latter access

to their online services. The protocol may be used by the other public services only if they hold the relevant authorisations delivered by the Sectoral Committee of the National Register.

At all times, the end user is free to terminate the processing of the personal details entered by him/her by signing out.

The privacy audit trail sees to it that logins and attempted logins may be reconstructed with a view to complying with the statutory obligation (article 16§4 of the Act of 8 December 1992) to appropriately protect the personal details.

Powered by FOD Beleid en Ondersteuning – DG Digitale Transformatie uses cookies to enhance the performance of the website, functional cookies for raising the website's user-friendliness and temporary session cookies necessary for authentication purposes during the session. Users are free to refuse the cookies, in which case some parts or our websites may not work properly or not work at all.

Necessary cookies

These cookies are indispensable to check your identity with a view to ensuring security, and to give you access - pursuant to successful identification and authentication - to the applications you would like to have access too.

Functional cookies

Functional cookies are cookies that are aimed at improving the operation and user-friendliness of the websites. Powered by FOD Beleid en Ondersteuning – DG Digitale Transformatie uses cookies to keep track of your language preferences.

Cookies for website performance

Powered by FOD Beleid en Ondersteuning – DG Digitale Transformatie uses load balancing cookies. These cookies are used on websites that attract a lot of visitors with a view to distributing the load of the many requests across several, separate networks and servers.

Cookies can be refused in the browser settings.

Article 8 - Definitions

For the purposes of the present terms of use, the concepts below are to be understood in the manner as specified:

- **Registration** - The process whereby a person has his/her name included on a list – by complying with a compulsory procedure -, and thereby lets is be known that he/she wishes to use a specific service.
- **Identification** - A process that is used to ascertain the identity of a specific person.
- **Authentication** – A process that is used to confirm the identity of a specific person. By providing certain confidential details that are known only to him/her (e.g. a password chosen by him/her), that person is able to confirm that he/she is in fact the person he/she claims to be.