Data protection notice regarding the user access management of the healthdata.be applications and its service desk functions

It is important that your data is properly secured. We handle it carefully and follow the data protection laws, such as the General Data Protection Regulation (GDPR).

Why do we collect and store your personal data?

We use your personal data to authenticate you as a mandated user of one or more of the healthdata.be applications or tools

- HD4DP: *an application enabling caregivers (e.g. hospitals, labs) to locally collect data and securely transfer these data towards the healthdata.be platform*
- HD4RES: *an application enabling researchers to monitor dataflows from the data providers*
- Healthdata.be Datawarehouse: *environment for research teams to store, validate and analyze the collected data*
- Healthstat: *an extranet environment to share reports with external actors (e.g. benchmarking reports for healthcare practitioners or public reports)*
- Healthdata.be EAM Portal: *a portal for healthcare organizations and/or individual healthcare practitioners to demand and/or validate access rights to HD4DP and/or Healthstat*
- Healthdata.be Service and Support portal: *created for users to request something or ask help in case of incidents concerning applications*

A secure user and access management helps to prevent (identity) fraud. Such prevention is important as the applications are linked to

a) the collection of patient data and/or healthcare providers data for policy-supporting research
b) access to (potentially sensitive) reports regarding the quality of healthcare actors and/or
c) support questions regarding the applications that could imply access to patient data or sensitive business data.

We also use your data to provide you with support for your service requests or issues with applications. Data might also be used to monitor or evaluate our support services.

Additionally, we could utilize your gathered data to communicate relevant information about the projects you are involved and its used applications. For instance: invitations for webinars or meetings about the project, key message about the project *(e.g. start date of data collections, technical interruptions)* or mailings related to project changes.

Who is responsible for processing your personal data?

The applications are managed by the Sciensano service healthdata.be.

Healthdata.be's mission is to facilitate the data exchange between healthcare professionals and researchers to increase public health knowledge and to adjust health care policy, with respect for the privacy of the patient, the healthcare professional and the medical confidentiality.

Healthdata.be is a service of Sciensano. Sciensano is a public institution with legal personality established by the Act of 25 February 2018 regarding the establishment of Sciensano, with registered office at rue Juliette Wytsman 14, B-1050 Ixelles and registered with the Crossroads Bank for Enterprises under the number 0693.876.830.

What is the legal basis for this processing?

Sciensano processes your personal data based on:

- Legitimate interest (art. 6 § 1 f) GDPR

As mentioned the processing is linked to manage the usage of applications. Your personal data facilitates

a) the creation and maintenance of access rights to applications you need to use because of voluntary or compulsory involvement in a scientific, policy-support healthcare project and
b) the provision of support to users having questions or issues related to the applications.

Which personal data is processed?

The following personal data can be processed:

- Your social security number (for access to the Healthdata.be Service and Support portal or Healthstat with support of Federal Authentication Services[1], eIDAS[2] and/or eHealth IAM service[3])
- Surname and first name
- Your professional number in you are a healthcare professional (for access to Healthstat with support of eHealth IAM service)
- Your e-mail address and your telephone number
- Membership of an organization that uses healthdata.be applications (e.g. a hospital, a lab, a research institution, …)
- Login credential information (e.g. user name, password)
- Involvement in a research project

How do we obtain your data?

We can receive your data directly from you when you have

a) submitted a request via the Healthdata.be Service and Support portal and/or the EAM Portal
b) contacted us via other communication channels (e.g. e-mail)

In other cases your data might be delivered to healthdata.be via the Access Manager of your healthcare organization[4] or via a project responsible that provides us a list of actors needing to have access to healthdata.be applications for their project.

---

[1] Via the Federal Authentication Service (FAS) individuals are authenticated so that they can access secure online government applications. Source: https://dt.bosa.be/en/identificatie_beveiliging/federal_authentication_service

[2] eIDAS stands for "Electronic Identification And Trust Services" and refers to the European legislation "Regulation (EU) 910/2014". This legislation aims to facilitate "cross-border digital transactions (interoperability) between citizens of the European Union, in order to stimulate economic and social development between the participating countries". What are the practical implications of eIDAS for users?

- Using their eID (or electronic foreigner's card for non-Belgian residents) or itsme®, Belgian citizens can log into an online service of another European country.
- Citizens of another European country can use their own (notified) national identification and authentication means to log into online services of Belgian authorities.

Source: https://sma-help.bosa.belgium.be/en/eidas#7258

[3] The eHealth platform, a public institute, provides a range of informatics tools like integrated identity and access management (IAM). These free tools can be freely integrated in a medical data management software package, in a data server or any other application (online service) whose user is an actor in the health sector. Their IAM service ensures that only authorized healthcare providers/institutions can access the services they are authorized to access.

[4] Depending on the healthcare organization this could be someone from your IT department, a VTE/RAE, an administrative staff member, … that has been assigned to validate access rights related to healthdata.be applications for your organization

To whom may your data be disclosed?

Personal data collected will be treated confidentially. They will only be used in the context of the aforementioned purposes.

The following categories of recipients of (certain) personal data are:

- processors to which the Sciensano service of healthdata.be appeals for secured storage or secured transfers of data
- the ICT services of your hospital or lab for coordination of healtdata.be matters at the healthcare facility level
- project owners that use the healthdata.be application for their research project

Healthdata.be has several customers who purchase services from it for their scientific, policy-supporting research projects including:

- Researchers from the Sciensano Department Epidemiology
- Health administrations such as the RIZIV-INAMI and the FPS Public Health/SPF Santé Publique
- Universities
- Pharmaceutical companies in the context of Managed Entry Agreements
- Scientific associations on a particular health issue

A project owner might receive your identity and/or contact data to follow-up the onboarding process of his/her project or to communicate with you about practical matters concerning the project.

Sciensano will not provide personal data to third parties for direct marketing purposes. Sciensano will not disclose personal data to third parties who are not part of the aforementioned recipients.

Processors

Healthdata.be calls upon processors for services/products concerning the secured storage or transfer of your data.

The services of following actors are used for following processing activities

- Dropbox: digital work environment to store and share internally documentation related to project management (e.g. stakeholders mapping)
- ServiceNow: ticketing system to capture, store, treat, follow-up and evaluate your requests or incidents involving the healthdata.be applications
- Salesforce: tool at Sciensano to manage customer data such contact details of users of our applications
- Microsoft (Azure Messaging ServiceBus): to facilitate the transfers of credentials to hospital or lab users
- Cronos Public Services: providing services to host data

Will your data be communicated to countries outside the European Economic Area (EEA)?

Both for its own applications and applications from sub-processors, Sciensano chooses servers located within the EEA. However, although maybe less applicable for the healthdata.be use cases, it cannot be excluded that certain US sub-processors in exceptional cases might be forced by US government to process particular data outside the EEA due to US regulations related to national security or justice affairs.

For more information on how these firms deal with US government requests:

- See policy Dropbox: https://help.dropbox.com/transparency

- See policy Salesforce: https://www.salesforce.com/content/dam/web/en_us/www/documents/legal/salesforces-principles-for-government-requests-for-customer-data.pdf
- See policy ServiceNow: https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/legal/data-processing-addendum.pdf
- See policy Microsoft: https://www.microsoft.com/en-us/trust-center/privacy

How long do we keep your personal data?

Access to the applications is linked to policy-supporting, scientific health (care) projects. Your data will be kept at least as long as the project is running and the applications are used for the project. You or the access manager within your organization can ask to stop the access at any time (e.g. when leaving the organization or ending involvement in a project).

Even when the project ends, Sciensano may still retain certain data in the context of evaluations of the project, the possibility of audit controls or archiving obligations for public administrations. Reasonable retention periods are taken into account in accordance with objective guidelines (e.g. the minimum standards of the Crossroads Bank for Social Security).

What are your rights?

These are your legal rights:

- You have the right to be informed properly about what happens to your personal data
- You have the right to access your personal data. You can obtain a copy of your data.
- Is your data incorrect? Then we have to correct it.
- You have the right to obtain the erasure of your personal data in certain circumstances.
- You have the right to object to the processing of your personal data in certain circumstances.

How do I file a complaint?

Without prejudice to the above regarding who to contact to exercise your rights, you can address any questions or complaints to the data protection officer (DPO) of Sciensano via

- dpo@sciensano.be or
- the following webform https://www.sciensano.be/en/privacy-notice-sciensano

You can also lodge a complaint with the Data Protection Authority (e-mail: contact@apd-gba.be). For more information about this authority: https://www.dataprotectionauthority.be/citizen

Modifications

We may amend this privacy statement as required. For example, if there are changes with regard to the personal data (sub)processors, or if the list of processed personal data changes.

This policy was last updated on 28 August 2023.