

EUROPEAN HEALTH DATA SPACE

Secure Processing Environments

The protected workspace where approved analysis happens — and the safeguards that surround it.



THE GOVERNMENT
OF THE GRAND DUCHY OF LUXEMBOURG
Ministry for Digitalisation

Government commission for data sovereignty

Supported by  **LNDS**



**Co-funded by
the European Union**

Scope

Key elements.

01

What an SPE is, and why it exists

A protected workspace for
analysis under defined conditions.

02

How access is authorised

Each request is checked.
A permit is granted only if all
conditions are met.

03

How the SPE keeps data protected

Personal access, logging, no
copies, audits, output review.

PART ONE

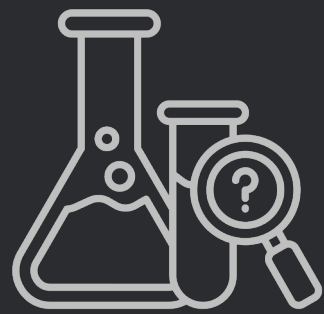
Why the SPE exists

Health data carries real public value and real sensitivity.
The SPE is how both are held at once.

01

Why secondary use needs protection

WHEN RE-USED RESPONSIBLY, HEALTH DATA CAN SUPPORT



Research



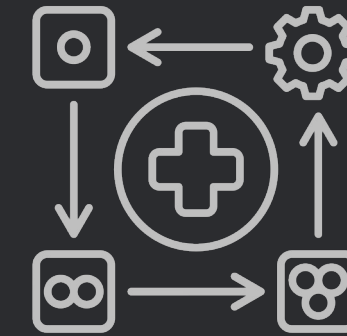
Innovation



Education



Public health



Policy design



**Official
statistics**

BUT

**Data must always be handled
securely and responsibly.**

Health data can reveal information about individuals, or be protected by intellectual property rights. That is why it can only be re-used within an SPE.

A protected digital workspace

Approved researchers, innovators, or public authorities analyse health data without taking it out of the secure system.

LIKE A LIBRARY READING ROOM

You can read a rare document and take notes, under supervision. You cannot walk away with the original.

In the EHDS process, this secure workspace is called a **Secure Processing Environment**, or **SPE**.



THE RISKS IT REDUCES

Unauthorised access

Access is limited to authorised users.

Misuse of data

Use takes place under the permit conditions.

Unsafe data release

Results are checked before release.

SPE: Before, during, after



GOES IN

Project data prepared under the permit conditions

Pseudonymised or anonymised, combined where approved.



SECURE PROCESSING ENVIRONMENT

Checks active

Activity logged and monitored

Authorised users work inside

Only authorised users, and each access is personal.
It cannot be passed on.

The data never leaves

No copies, no downloads, only in-SPE analysis.



GOES OUT

Only disclosure-controlled, anonymised outputs

Reviewed by the CGSD
before release.

PART TWO

How access is decided

Before anyone can re-use health data,
strict checks take place.

02

From discovery to application

The discovery stage starts in the National Health Datasets Catalogue and ends with a formal application, not directly with data.

01

Find relevant datasets

In the National Health Datasets Catalogue.



02

Prepare a formal request

Purpose, expected outcome, and the specifications that follow.



03

Submit to the CGSD

The dossier enters formal review.

STATUS No access has been granted yet.

What the application must specify

Four specifications make the processing privacy-preserving and technically feasible.

A

Purpose and expected outcome

What the project is for, and the public value it is expected to produce.

B

Data scope

Data type, time range, and sources. This should never be more than the project really needs.

C

Data format justification

Why anonymised or pseudonymised data is needed.

D

SPE analysis setup

The technical tools and computational power the analysis will require.

Every request is reviewed individually

The Government Commission for Data Sovereignty (CGSD), as the Health Data Access Body (HDAB), carries out a consistent series of checks.



Is the requested data necessary?

Access is limited to what the project genuinely needs.

+



Is the objective allowed?

Checked against the purposes permitted by European rules.

+



Are data subjects' rights protected?

The proposed setup is adequate for secure processing.

THE CONDITION

A permit is only granted if all the conditions are met.



If they are, access is authorised through a data permit.

PART THREE

Permit-based provisioning

Having a permit doesn't mean getting direct access.
Two operational tasks come first.



03

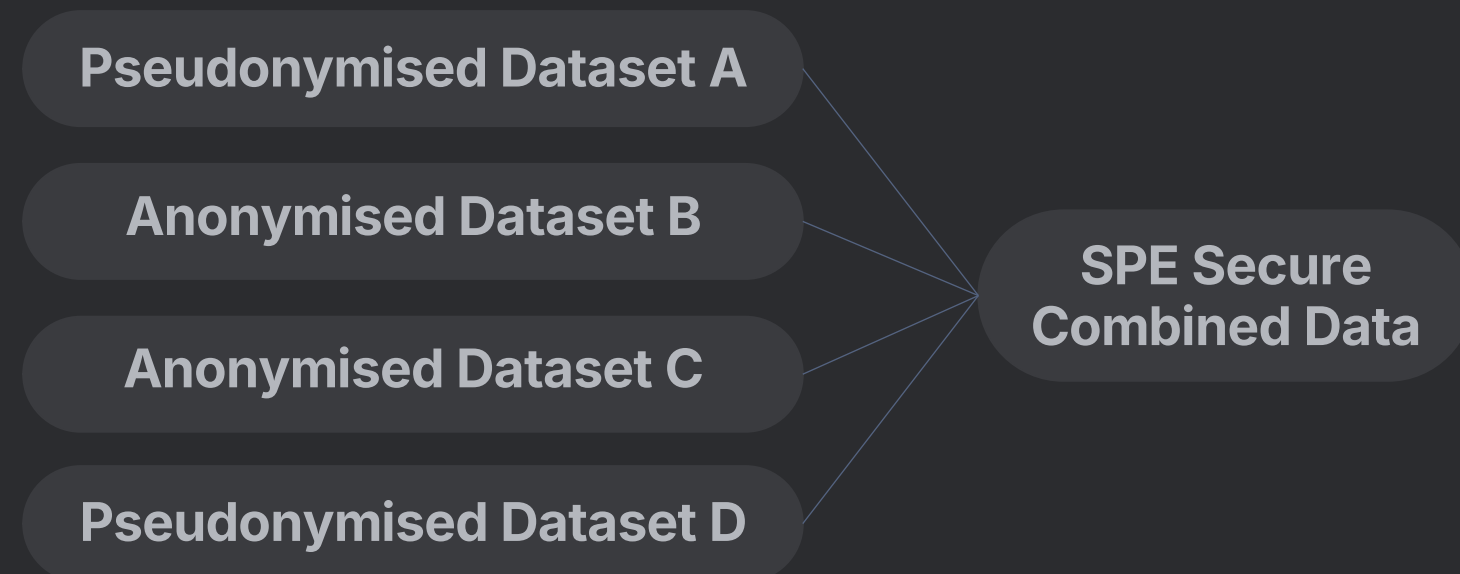
Two tasks before access

After a permit is granted, the CGSD puts security measures in place to protect the data and prevent misuse.

TASK ONE

Prepare the project data

Apply pseudonymisation or anonymisation measures, and combine datasets where approved.



TASK TWO

Make it available in the SPE

The prepared data is placed in a Secure Processing Environment configured according to the permit.

- + Prepared project data
- + Authorised tools
- + Required compute resources

✓ Only then can authorised users connect and analyse data.

PART FOUR

Governed use, controlled output

What happens inside the environment,
and what is allowed to leave it.

04

How the SPE protects data

Protection is a property of the system, not a judgement about the people using it.



ACCESS

Authorised and personal

Only specifically approved people can get to the data.
Access rights cannot be passed on to someone else.



CONTAINMENT

Data stays in the protected system

Data cannot be copied, downloaded or shared.



TECHNICAL CHECKS

Continuous technical checks

What is accessed is matched against what was approved.



TRACEABILITY

Every action logged

Anything unusual can be spotted and traced afterwards.

AND OVER ALL OF IT **The whole system is regularly reviewed and audited.**

Nothing leaves without review

Results are not exported by the researcher. They are requested, checked, and released by the CGSD.

01

Approved activity

Analysis runs inside the SPE, within the permit's scope.



02

Proposed output

The user submits an export request to the CGSD.



03

CGSD review

Disclosure control and anonymisation requirements are checked.



04

Approved output released

Approved anonymised output leaves the SPE. The data stays inside.



Only outputs that pass disclosure control and meet anonymisation requirements can be exported.

IN CONCLUSION

The SPE turns access rules into practical safeguards.

It enables secondary use of health data in a controlled and secure way, supporting analysis while keeping strong protection around sensitive data.

THANK YOU

Questions

RELATED TRAINING ASSETS

What is EHDS?

What is HDAB?

What secondary use makes possible

Discovering datasets in the catalogue

Health data holder obligations



THE GOVERNMENT
OF THE GRAND DUCHY OF LUXEMBOURG
Ministry for Digitalisation

Government commission for data sovereignty

This presentation is provided for information purposes only and is not intended to be exhaustive. It does not necessarily reflect the position of the CGSD and should not be construed as constituting an official position of the CGSD. The information and views expressed in this presentation are without prejudice to any future position, decision or action of the CGSD and do not create any commitment or obligation on its part.



**Co-funded by
the European Union**

Co-funded by the European Union. Views and opinions expressed are, however, those of the authors only and do not necessarily reflect those of the European Union or HaDEA. Neither the European Union nor the granting authority can be held responsible for them.