



User Guide

—

Application for re-use of data



THE GOVERNMENT
OF THE GRAND DUCHY OF LUXEMBOURG
Ministry for Digitalisation

Government commission for data sovereignty

Publication date: 13/07/2026

Table of Contents

1	Introduction	3
2	Definitions	4
3	Identification of PSB Data	6
3.1	Where can I find information about the PSB Data that may be subject to an Application for Re-Use of Data?	6
3.1.1	In the Catalogue	6
3.1.2	Directly with the Data Holder	7
3.2	The grounds for protection of the PSB Data	7
3.2.1	Personal data	7
3.2.2	Protection of the intellectual property rights of third parties	9
3.2.3	Protection of commercial confidentiality and trade secrets	9
3.2.4	Protection of statistical confidentiality.....	11
3.3	Determination of data excluded from the scope of the DGA.....	11
3.3.1	Data held by state-owned enterprises	11
3.3.2	Data held by public service broadcasters.....	11
3.3.3	Data held by cultural establishments.....	11
3.3.4	Data held by educational establishments	12
3.3.5	Data protected for reasons of public security, defence or national security	12
3.3.6	Data exchanged between PSB for the sole purpose of carrying out their public service mission	12
3.3.7	Data obtained on the basis of Chapter V of Regulation (EU) 2023/2854 (Data Act)	12
4	Creation and certification of the business eSpace.....	13
5	Preparing your Application for Re-Use of Data	14
5.1	Information	15
5.2	Contact point	16
5.3	Applicant(s)	17
5.4	Data Holder(s) of the PSB Data	19
5.5	Description of the context of access to and re-use of data	20
5.5.1	Context of your Application for Re-Use of Data	20
5.5.2	Objectives of your Application for Re-Use of Data.....	20
5.5.3	Purposes	20
5.5.4	Justification of the proportionality of the Application for Re-Use of Data.....	23
5.6	Description of data categories	23
5.6.1	The grounds for protection of PSB Data	23

5.6.2	Special categories of Personal Data	24
5.6.3	External Data	24
5.6.4	Data format	24
5.6.5	Detailed description of the necessity and proportionality of the requested data	25
5.6.6	Annex: "Data Description"	25
5.7	Lawfulness	34
5.7.1	Lawful conditions for processing under Article 6 of the GDPR	34
5.7.2	Special categories of personal data pursuant to Article 9 of the GDPR	37
5.8	Appropriate Measures Plan	40
5.8.1	Purpose of the template	40
5.8.2	Final checklist and resources	41
5.9	Duration	42
5.9.1	Authorised Duration	42
5.9.2	Archival period	42
5.9.3	Justification of data use and retention periods	42
5.10	Users	43
5.11	Rights and freedoms	44
5.12	Secure Processing Environment (ETS)	45
5.12.1	Internal Technological Solutions	45
5.12.2	Addition of External Technological Solutions	45
5.13	Validation and signatures	47
5.14	Attachments	48
6	Submitting the Application for Re-Use of Data and the assessment by the CGSD	50
6.1	Submitting the Application for Re-Use of Data	50
6.2	Assessment by the CGSD	50
6.3	Duration of assessment of the Application for Re-Use of Data	51
6.4	Request for additional information	51
7	Decision of the CGSD	52
7.1	Adoption and notification of the decision	52
7.2	Publication of the decision	52

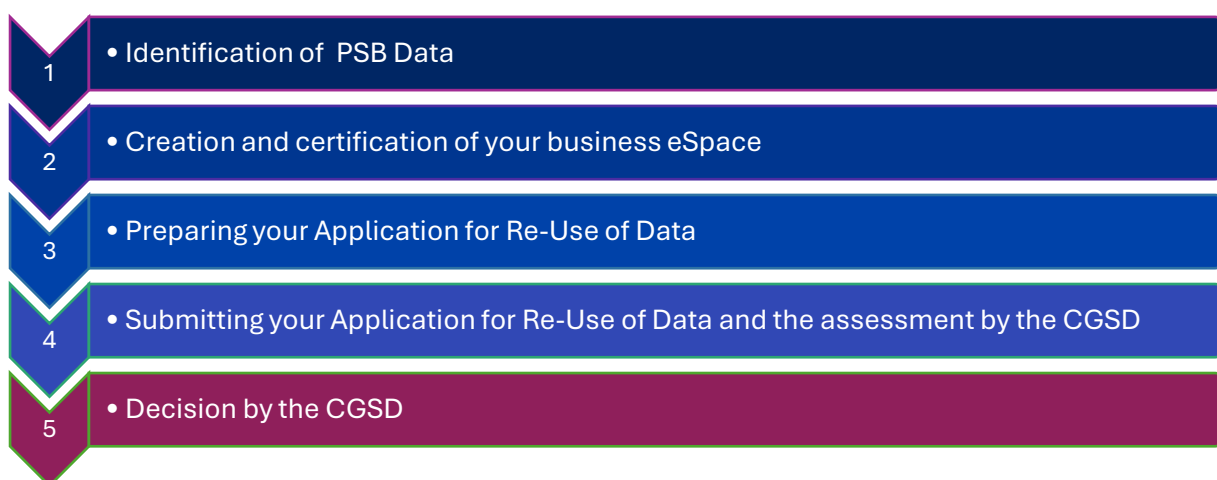
1 Introduction

This guide (hereinafter referred to as the "User Guide") aims to accompany you, after [the certification of your business eSpace](#), in the context of your Application for Re-Use of Data.

You will find:

- a presentation of the various steps required to submit your Application for Re-Use of Data,
- practical advice, and
- useful information regarding the processing of your Application for Re-Use of Data.

General presentation of the process of an Application for Re-Use of Data



△ The preparation of the Application for Re-Use of Data requires time and input from the Public Sector Body holding the data requested.

If necessary, you will also need to consult the Data Protection Officer (DPO) and the Chief Information Security Officer (CISO) of your organisation.

If you wish, you may also request the assistance of the LNDS when preparing your application.

△ This User Guide is provided for informational and educational purposes only. Its objective is to assist Applicants when preparing the Application for Re-Use of Data and filing it, without however constituting a document with normative or legally binding value.

Although utmost care has been taken in drafting it, no guarantee is given as to the accuracy, completeness or timeliness of the information contained therein. The content of this User Guide may be amended, supplemented or updated at any time, in particular to take account of changes in the procedure, IT tools or the applicable legal and regulatory framework.

The information provided in this User Guide is without prejudice to the laws and legal provisions applicable in this area, including in particular Regulation (EU) 2022/868 on data governance, the Law of 19 December 2025 establishing the Government Commission of data sovereignty, and the [general terms of use of the secure IT environment \(SIE\)](#). In the event of any discrepancy between this User Guide and the aforementioned legal texts, the latter shall prevail.

2 Definitions

The terms used in this User Guide are defined as follows, whether they are used in the singular or plural:

“Applicant”: the natural or legal person, including a public authority, a service or any other public sector body, who submits an Application for Re-Use of Data to the CGSD in order to obtain an Authorisation.

“Application for certification”: an application by an Applicant for certification of the MyGuichet.lu business eSpace.

“Application for Re-Use of Data”: an application lodged by one or more Applicants to obtain an Authorisation in accordance with the Law.

“Appropriate Measures”: measures proposed by the Applicant in the Appropriate Measures Plan. These may include measures such as anonymisation and/or pseudonymisation of the data, as well as modification, aggregation, deletion, or treatment using any other data disclosure control method. These measures are intended to ensure compliance with and the protection of the relevant rights and interests (without limitation), including data protection, intellectual property rights, commercial confidentiality (including trade secrets), professional secrecy, business confidentiality, statistical confidentiality, third-party rights, and the confidentiality of data.

“Appropriate Measures Plan”: the document in which the Appropriate Measures proposed by the Applicant are described.

“Authorisation”: an authorisation for re-use of Target Data issued by the CGSD following an Application for Re-Use of Data.

“Authorised Duration”: the period during which the Applicant is authorised to access or use the SPE and the Target Data in accordance with the Authorisation.

“Catalogue”: the public sector data catalogue, which includes descriptions of datasets, including PSB Datasets and open datasets, that are only visible to the general public (excluding descriptions of datasets that are only visible to specific state actors).

“CGSD”: the Government Commission for data sovereignty within the meaning of the Law.

“CTIE”: the Government IT Centre established by the Law of 20 April 2009 establishing the Government IT Centre.

“Data Holder”: a Public Sector Body holding PSB Data.

“Data Subject”: an identified or identifiable natural person within the meaning of the GDPR.

“DGA”: Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance (Data Governance Act).

“DPIA”: a data protection impact assessment within the meaning of Article 35 of the GDPR.

“External data”: any data which does not fall within the scope of the PSB Data and which the Applicant wishes to have made available in the SPE, in addition to or in combination with the PSB Data, as such data may come from third-party, open or private sources.

“External Technological Solution”: the software, algorithms, artificial intelligence models, systems and tools covered by the Authorisation provided by the Re-User for integration into the SPE.

“GDPR”: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and

on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

“Internal Technological Solution”: the software, algorithms, artificial intelligence models, systems and tools provided as standard solutions in the SPE by the CGSD.

“Law”: the Law of 19 December 2025 establishing the Government Commission for data sovereignty.

“LNDS”: the Luxembourg National Data Service: www.lnds.lu. **“PSB Data”**: data held by a Data Holder.

“Personal data”: personal data, namely any information relating to an identified or identifiable natural person as defined in Article 4(1) of the GDPR.

“Public Sector Body” or **“PSB”**: the State, regional or local authorities, bodies governed by public law or associations formed by one or more such authorities, or one or more such bodies governed by public law.

“State”: the State of the Grand Duchy of Luxembourg.

“SPE”: the secure processing environment.

“Target Data”: PSB Data, and where applicable, External Data, to which Appropriate Measures and possibly additional measures have been applied by the CGSD following an Authorisation and before being made available in the SPE.

“Working Data”: data that has been produced in the SPE by the Re-User from the Target Data.

“User”: any natural person authorised to use the SPE in accordance with the Authorisation.

3 Identification of PSB Data



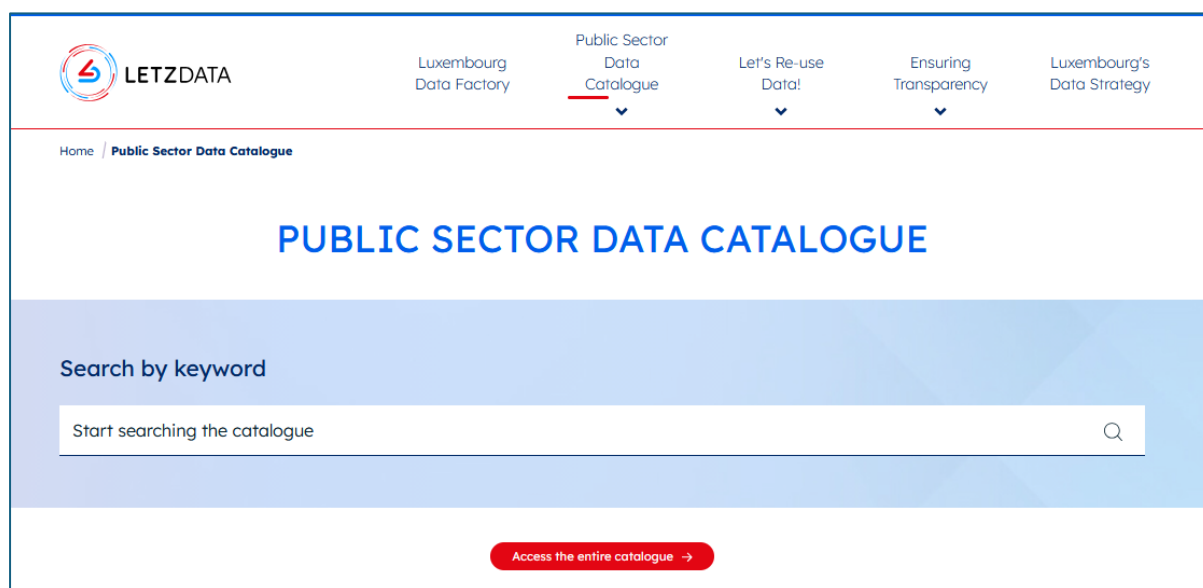
When preparing your Application for Re-Use of Data, you should first identify the PSB Data you need by:

- determining which PSB holds the PSB Data you require (section 3.1),
- verifying that the PSB Data may be subject to an Application for Re-Use of Data (Section 3.2),
- verifying that the PSB Data is not excluded from the scope of the DGA (section 3.3).

If you wish to combine the requested PSB Data with External Data, please specify this in the Data Description (section 5.6.6).

3.1 Where can I find information about the PSB Data that may be subject to an Application for Re-Use of Data?

3.1.1 In the Catalogue



[The Catalogue](#) describes the PSB Data that may be subject to an Application for Re-Use of Data. It does not provide access to the data itself, but provides useful information, including:

- the type of PSB Data,
- the format of the PSB Data,
- conditions and access restrictions applicable to the PSB Data.

If you require additional information regarding PSB Data, or if you wish to discuss the extent of their availability, you may contact the relevant Data Holder using the contact details provided in the Catalogue.

The agreement of the Data Holder for your project is essential, including where all access conditions or usage criteria are published in the Catalogue. The Data Holder grants its formal agreement to the project through the signature of the Application for re-use of data.

⇒ The Catalogue also refers to unprotected datasets, known as “open data”.

If your Application for Re-Use of Data involves combining open data with PSD Data, list the open data as “External Data” in the Application for Re-Use of Data.

For more information on open data, see [Home - Open Data Portal](#).

3.1.2 Directly with the Data Holder

If the PSB Data you are looking for does not appear in the Catalogue, you can contact the relevant Data Holder directly.

If you are unsure which Data Holder is responsible for a particular dataset, or if you have any questions about datasets, the [Ministry for Digitalisation](#) may assist you by redirecting you to the appropriate Data Holder.

3.2 The grounds for protection of the PSB Data

PSB Data available for Re-Use may be protected on the basis of:

- the [protection of personal data](#),
- the [protection of the intellectual property rights of third parties](#),
- [commercial confidentiality, including trade, professional and business secrets](#),
- [statistical confidentiality](#).

As a general rule, the applicable protection grounds for PSB Data are indicated in the Catalogue.

3.2.1 Personal data

3.2.1.1 General elements

Personal Data may be **directly** or **indirectly identifiable**.

It is **directly identifiable** where it enables a natural person to be identified immediately, such as a name, surname or an e-mail address in an individual's name.

It is **indirectly identifiable** where, on its own, it does not identify an individual but may do so when combined with other information (for example: an internal identifier, postal address, telephone number, customer number or a specific employment start date). While certain data may not, in isolation, reveal the identity of an individual, they may still constitute Personal Data if their combination with other information allows the Data Subject to be identified unambiguously.

Furthermore, whether data qualifies as Personal Data does not depend on its level of confidentiality. Information that is publicly available may still be considered Personal Data if it enables the direct or indirect identification of a Data Subject.

Finally, where a dataset contains both Personal Data and non-personal data that are inextricably linked, data protection obligations applicable to Personal Data apply to the dataset as a whole.

Personal Data may fall within the **Special Categories of Personal Data**, which are subject to additional conditions under the GDPR. This is the case for processing:

- revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership (for example: membership of a political party, participation in political meetings, religious affiliation, or information relating to spiritual practices or deeply held moral beliefs)
- of genetic data, such as DNA analyses or hereditary characteristics;
- of biometric data processed for the purpose of uniquely identifying a natural person, such as fingerprints, facial recognition data, iris scans, voiceprints, or other physiological or behavioural characteristics enabling unique identification;
- of data concerning health, including information on physical or mental health status, medical records, treatments, disabilities, test results, or data generated by connected medical devices; and
- of data concerning a natural person's sex life or sexual orientation.

*The processing of **Personal Data** within the SPE*

In this case, the following factors must be borne in mind:

- the Applicant will qualify as the controller under Article 4 of the GDPR for processing activities carried out within the SPE; and
- where several Applicants jointly submit an Application for Re-use of Data, those Applicants will be considered joint controllers under Article 26 of the GDPR. In such cases, the Applicants must put in place arrangement setting out, in a transparent manner, their respective responsibilities for compliance with GDPR obligations (for example: drafting and providing the data protection notice, determining responsibility for notifying the National Commission for Data Protection (CNPD) in the event of a personal data breach, or carrying out a Data Protection Impact Assessment, where applicable).

For more information on the obligations of controllers, including joint controllers, please see:

https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_fr

For more information on Personal Data, see:

- [Opinion 04/2007 of the Article 29 Working Party on the concept of personal data](#)
- [Thematic factsheet of the Court of Justice of the European Union on the protection of Personal Data \(07/2024\)](#)

3.2.1.2 Non-personal data and anonymised data

Non-personal data and anonymised data are not subject to Personal Data protection rules.

Non-personal data refers to information that does not relate to a Data Subject, such as the postal address of a public authority, a general contact telephone number, or weather data. Such information does not enable an individual to be identified and is therefore not considered Personal Data.

Anonymisation is the process of irreversibly transforming Personal Data so that a Data Subject can no longer be identified, whether directly or indirectly, by any means reasonably likely to be used. Once data has been properly anonymised, it is no longer considered Personal Data.

For more information about pseudonymised data, see:

- [Opinion 05/2014 of the Article 29 Working Party on Anonymisation Techniques](#)
- [EDPS Guidelines 01/2025 on pseudonymisation](#) (update ongoing)

3.2.1.3 Pseudonymised data

Pseudonymisation of Personal Data is a process of substituting directly identifying data (e.g. surname, first name, etc.) with indirectly identifying data (e.g. alias, sequential number, etc.). This process makes it possible to process data of individuals without being able to identify them directly. Pseudonymisation is a reversible process (unlike anonymisation). Indeed, it is possible to re-identify individuals if additional information is available. Pseudonymised data therefore remain, in theory, subject to the obligations of the GDPR.

For more information about pseudonymised data, see:

- [Opinion 05/2014 of the Article 29 Working Party on Anonymisation Techniques](#)
- [EDPS Guidelines 01/2025 on pseudonymisation](#) (update ongoing)

3.2.2 Protection of the intellectual property rights of third parties

PSB Data and External Data may be protected by:

- literary and artistic property rights, including copyright, neighbouring rights (e.g. performers, producers) as well as database rights,
- industrial property rights, including trademarks, patents (and other associated rights) and designs.

When the PSB Data or External Data covered by your Application for Re-Use of Data is protected by the intellectual property rights of third parties, it is your responsibility to verify the applicable conditions governing their re-use. Such re-use may, for example, be subject to the payment of royalties or fees.

3.2.3 Protection of commercial confidentiality and trade secrets

3.2.3.1 Confidential information¹

Confidential business data is defined as data that meets all three of the following cumulative conditions:

- the data is known only to a limited number of people. In that regard, information may lose its confidential nature where it becomes available to specialist circles or capable of being inferred from publicly available information;²
- the disclosure of the information is likely to cause serious harm to the person who provided it or to third parties. The assessment of this risk is notably based on:

¹ Communication from the Commission on the protection of confidential information by national courts in proceedings for the implementation of EU competition rules on the initiative of the private sphere (2020/C 242/01), point 20 (2020 Communication).

² 2020 Communication, point 21.

- the nature of the information: information of commercial, financial or strategic value is generally considered to be particularly sensitive and likely to cause serious harm if disclosed;
- their recent nature: commercially sensitive information, such as information about an ongoing or future business relationship, internal company plans, or other forward-looking business data, could often qualify as confidential. However, that confidential nature may disappear if that information has lost its commercial importance due to the passage of time; and
- the interests liable to be harmed by the disclosure of the confidential information are, objectively, worthy of protection. That assessment is made on a case-by-case basis.³

Unlike a trade secret, the data holder is not required to have put in place specific reasonable measures to ensure the confidentiality of the information. Information will be considered confidential, if the interest in keeping it secret outweighs the public interest in transparency.

3.2.3.2 Trade secrets

To qualify as a trade secret, information must meet all three of the following conditions:

- it must be secret (i.e. not generally known or not readily accessible to persons within the relevant sector),
- it has commercial value because it is secret, and
- it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret⁴.

For example, trade secrets may protect:

⇒ technical information, such as manufacturing processes, pharmaceutical test data, designs and graphical representations of computer programs	⇒ commercial information, such as distribution methods, suppliers and customers lists and advertising strategies
⇒ information constituting know-how, such as manufacturing processes, commercial techniques or management methods	⇒ combinations of publicly available elements where their aggregation provides a competitive advantage .

3.2.3.3 Protection of professional secrecy

Professional secrecy, within the meaning of Article 458(1) of the Criminal Code, applies only to persons who are legally bound by such confidentiality obligations, including doctors, surgeons, health officers, pharmacists, midwives, lawyers, bankers, and journalists.

In Luxembourg, civil servants and other State employees are subject to an obligation of professional secrecy.⁵

³ Judgment of 30 May 2006, Bank Austria v Commission (T-198/03, EU:T:2006:136), para. 71.

⁴ Article 2 of the Law of 26 June 2019 on the protection of undisclosed know-how and business information (trade secrets) against unlawful acquisition, use and disclosure.

⁵ Article 11 of the amended Law of 16 April 1979 laying down the general statute for State officials, Article 1(3) and (5) for trainee civil servants and State employees. Article 6 of the State Employees Collective Agreement.

3.2.4 Protection of statistical confidentiality

Article 16 of the amended Law of 10 July 2011 on the organisation of the National Institute for Statistics and Economic Studies sets out the national framework for statistical confidentiality.

As such, data is considered confidential where it enables “*the direct or indirect identification of a natural or legal person or entail a risk of disclosure of individual information*”.⁶

When assessing whether a natural or legal person is identifiable, account must be taken of all means reasonably likely to be used by a third party to identify that person.⁷

3.3 Determination of data excluded from the scope of the DGA

The categories of data described in this section are excluded from the scope of the DGA and therefore cannot be the subject of an Application for Re-Use of Data.

3.3.1 Data held by state-owned enterprises

Data held by public undertakings falls outside the scope of the DGA and therefore cannot be the subject of an Application for Re-Use of Data.

A public undertaking is an undertaking over which PSBs may exercise, directly or indirectly, a dominant influence. Such influence is presumed in any of the following cases, if the PSB

- holds the majority of the undertaking’s subscribed capital,
- controls the majority of the votes attached to the shares issued by the undertaking, or
- can appoint more than half of the undertaking’s administrative, management or supervisory board.

In essence, an undertaking is considered to be “**controlled by the public sector**” where public authorities have the ability to determine its operations or strategic direction, through financial participation or governance rights.

3.3.2 Data held by public service broadcasters

Data held by public service broadcasters, their subsidiaries, and other bodies (and their subsidiaries, i.e. entities under their technical and de facto control) for the purpose of carrying out a public service broadcasting remit is also excluded.

Only data held for “**the fulfilment of a public service broadcasting remit**” falls outside the scope of the DGA. Accordingly, a Data Re-use Request may relate to data held by such broadcasters, bodies, or subsidiaries where that data is not used for the performance of the public service broadcasting remit, provided that it constitutes protected data in accordance with section 3.2 above.⁸

3.3.3 Data held by cultural establishments

Data held by, amongst others, libraries, archives, museums, orchestras, operas, ballets, and theatres is excluded from the scope of the DGA.

⁶ Article 16, second indent, of the amended Law of 10 July 2011 on the organisation of the National Institute of Statistics and Economic Studies.

⁷ Article 16, second indent, of the amended Law of 10 July 2011 on the organisation of the National Institute of Statistics and Economic Studies.

⁸ Para. 53 DGA, Article-By-Article Commentary, Specht/Hennemann, pp. 137-138.

In Luxembourg, the [list of cultural establishments made available by the Ministry of Culture](#) may provide more examples of cultural establishments.

3.3.4 Data held by educational establishments

Data held by educational establishments such as schools, colleges and universities does not, in principle, fall within the scope of the DGA.

By way of exception, the DGA may apply to data held where the establishment acts as a research-performing organisation.

However, the DGA does not apply to (i) data from collaborative research projects, in particular in the context of public-private partnerships; (ii) exchanges of data carried out exclusively in the context of public service missions, between public sector bodies within the Union or with public sector bodies from third countries or international organisations; and (iii) exchanges of data between researchers for the purposes of non-commercial scientific research.

3.3.5 Data protected for reasons of public security, defence or national security

Data protected for reasons of public security, defence or national security, including the data from procurement procedures falling within the scope of the Law of 26 December 2012 on defence and security procurement, is excluded from the scope of the DGA.

This exclusion applies to any type of Data Holder, provided that the data is protected for these reasons.

3.3.6 Data collected for activities other than those necessary for the carrying out their public task

Only data collected or produced in the context of the public task (consisting of specific administrative tasks) of a PSB may be applied for in the context of an Application for Re-Use of Data.

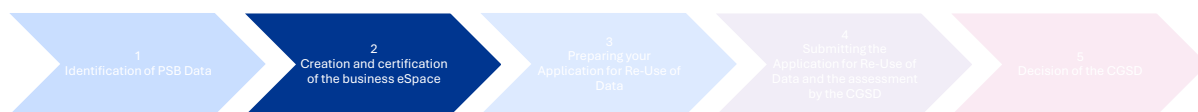
However, a PSB may carry out activities other than those necessary for the provision of a public task. For example, a non-profit organisation (*association à but non lucrative* - ASBL) may have a public task but may carry out other activities that do not fall within those tasks. Data collected in the context of these other activities are excluded from the scope of the DGA.

3.3.7 Data obtained on the basis of Chapter V of Regulation (EU) 2023/2854 (Data Act)

Data collected by a PSB for an exceptional need on the basis of Chapter V of Regulation (EU) 2023/2854 is excluded from the scope of the DGA,⁹ because they were obtained in a particular context (emergency, security, pandemic, natural disaster, etc.). The use of such data remains limited to address the exceptional need use for which they were collected.

⁹ Article 17(3) and recital 70 of Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act).

4 Creation and certification of the business eSpace

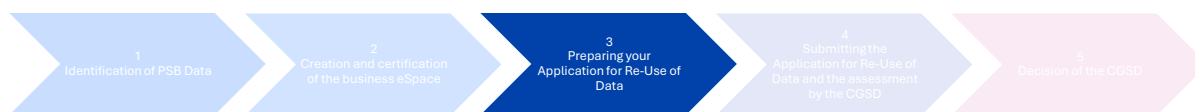


An Application for Re-Use of Data can only be submitted to the CGSD from your certified MyGuichet business eSpace.

The creation and certification of a MyGuichet business eSpace therefore constitute prerequisites for submitting an Application for Re-Use of Data.

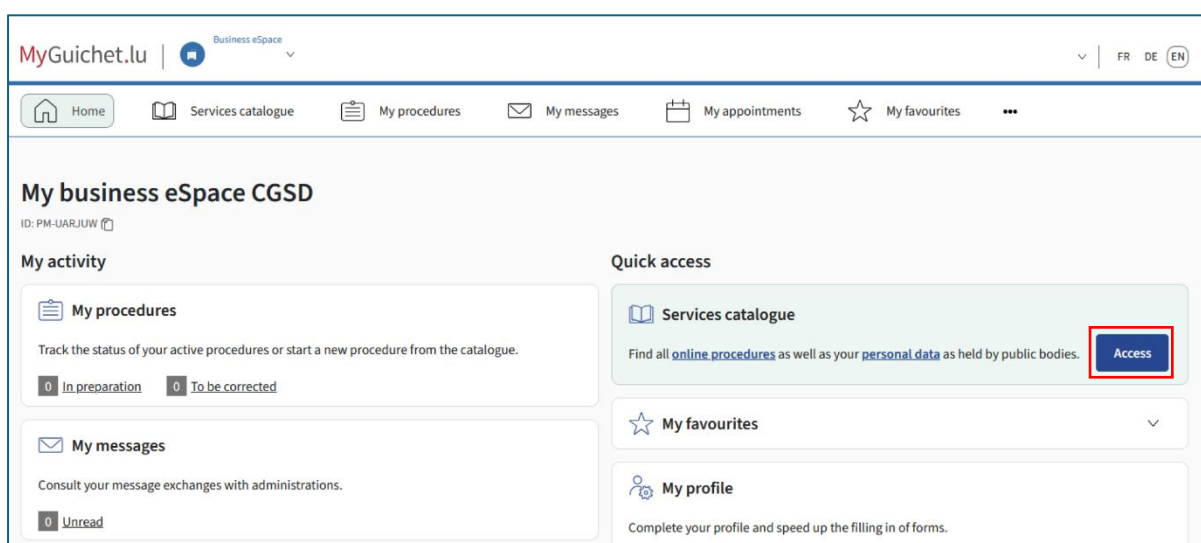
The various steps required to create a certified workspace are described in a separate guide entitled [User Guide - Creating a certified business eSpace.](#)

5 Preparing your Application for Re-Use of Data

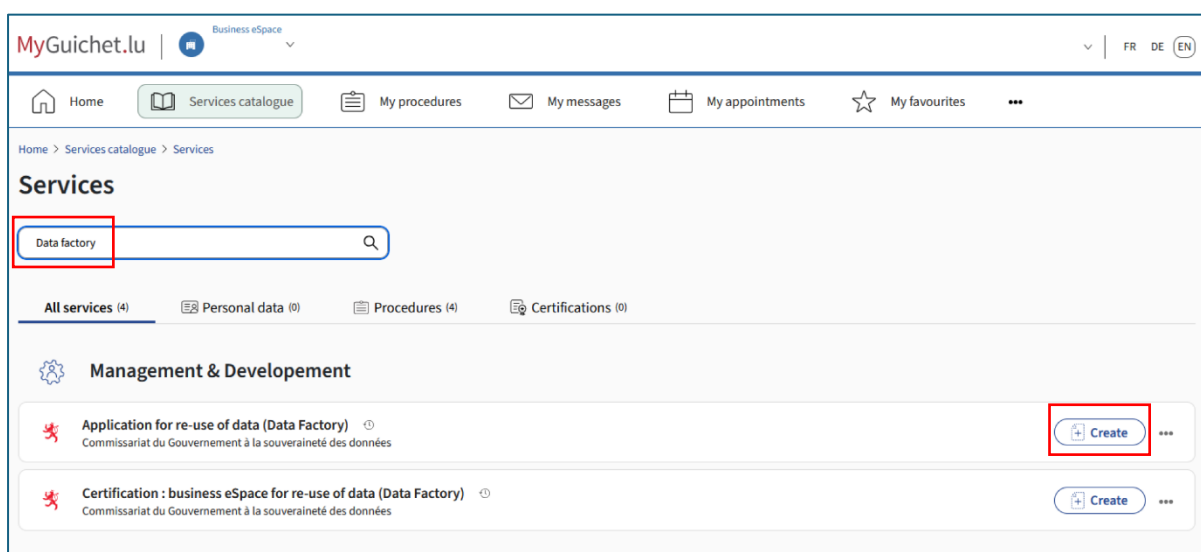


Once the CGSD has approved the certification of the business eSpace is validated, the procedure entitled "Application for Re-use of Data (Data Factory)" (referred to as the "Application for Re-Use of Data" in this User Guide) becomes visible and accessible in the search results of your MyGuichet.lu business eSpace. You can then fill in and submit the corresponding procedure as follows:

1. in your MyGuichet.lu certified business eSpace, click on "Access",



2. find the "Application for re-use of data (Data Factory)" procedure using the keywords "Data Factory" and start the procedure by clicking on the "Create" button,



3. complete the required information and submit your Application for Re-Use of Data as described below.

5.1 Information

Application for re-use of data (Data Factory)

Steps filling

Information

Contact person

Applicant(s)

Data Holder 1

Description of the context of access to and re-use of data

Description of data categories

Appropriate Measures

Data use and retention periods

Data users

Secure processing environment

Information

The purpose of this procedure is to enable the Applicant(s) to submit an application for access to and re-use of data to the Government Commission for Data Sovereignty (Commissariat du Gouvernement à la souveraineté des données - CGSD).

The CGSD, acting in its capacity as the controller pursuant to Regulation (EU) 2016/679 (GDPR), processes your personal data in order to manage applications for access to and re-use of data and to accept or refuse the applications in accordance with the law of 19 December 2025 establishing the Government Commission for Data Sovereignty (CGSD).

Your data is also processed for verification, analysis, statistical purposes as well as for evidence purposes and is retained for a period of thirty (30) years from the date of the CGSD's decision or, where applicable, from the end of the period of the access to and re-use of data authorised by the CGSD. If you do not provide the data indicated as obligatory, your application may be rejected.

You have the rights set out in Articles 12 to 22 of the GDPR as restricted by applicable legislation, including, under certain conditions, the right to object to the processing of your data. You also have the right to lodge a complaint with the National Commission for Data Protection (Commission nationale pour la protection des données) (www.cnpd.public.lu) located at 15, Boulevard du Jazz, L-4370 Belvaux.

If you have any questions relating to the processing of your data by the CGSD, please contact our data protection officer:

- by email: dpo@cgsd.etat.lu
- by post: DPO, Commissariat du Gouvernement à la souveraineté des données, 5, rue Plaetis, L-2338 Luxembourg.

A more detailed version of the information notice is [available here](#).

☐ By checking this box, you confirm that you have received and read the aforementioned information notice as well as the more detailed information notice relating to the processing of your personal data. *

*: mandatory field

Read the data protection notice and confirm having received and read both the short and the more detailed data protection notice concerning the processing of your personal data to proceed to the next step.

 LETZDATA

15

5.2 Contact point

Contact point

Étapes	Point de contact
Information ✓	Un seul point de contact peut être mentionné. Ce point de contact est chargé par le ou les Demandeur(s) de collecter l'ensemble des informations nécessaires auprès des différentes parties impliquées, y compris des Détenteurs de données. Il pourra être contacté directement par le CGSD aux fins d'obtenir des informations complémentaires. Point de contact ☐ Je suis le point de contact responsable pour l'introduction de la demande d'accès aux données et de leur réutilisation Prénom(s) * Nom * Rôle et fonction * E-mail professionnel * Veuillez ne pas indiquer une adresse électronique privée Téléphone professionnel ⓘ Veuillez ne pas indiquer un numéro de téléphone privé
Point de contact	
Demandeur(s)	
Détenteur de données 1	
Description du contexte de l'accès aux données et de leur réutilisation	
Description des catégories de données	
Mesures Appropriées	
Durées d'utilisation et de conservation des données	
Utilisateurs des données	
Environnement de traitement sécurisé	

The contact person, as the representative of the Applicant(s), is the primary contact for the CGSD. The contact person should be familiar with the operational aspects of the data re-use project and should be empowered to answer related questions. The contact person will be responsible for ensuring day-to-day communication and follow-up and must therefore be available and able to provide up-to-date information.

Where an Application for Re-Use of Data is submitted by several Applicants, one common contact person must be designated. This person will act as the primary contact for the Application and will ensure communication with all Applicants.

Assistance from the LNDS

Assistance from the LNDS
Did you receive assistance from the LNDS when preparing your application? * ☐ Yes ☐ No

Indicate whether the LNDS has assisted in preparing your application and, if so, provide the contact details of the LNDS contact person in the "LNDS Assistance" section. If you have obtained the assistance of the LNDS, this information makes it easier to process your Application for Re-Use of Data.

5.3 Applicant(s)

Steps filling	Applicant(s)
Information ✓	The information below has been pre-filled with the information certified by the CGSD.
Contact person ✓	
Applicant(s)	
Data Holder 1	
Description of the context of access to and re-use of data	
Description of data categories	
Appropriate Measures	
Data use and retention periods	
Data users	
Secure processing environment	

Applicant(s)
The information below has been pre-filled with the information certified by the CGSD.

Information concerning the entity
Name of the entity

Identification number

☐ The application is submitted jointly by multiple Applicants.
All Applicants must have a certified business eSpace for your application to advance

If the information that has been certified by the CGSD has changed (including a change to the person(s) with signing authority), the Applicant must submit a new certification request to the CGSD containing the amended information.

Person 1 with signing authority for the entity
First name(s)

Surname

Position held within the entity

☐ This person will not sign this application form for access to and re-use of data

Official address
Country

Postcode

Example: for L-2615, enter 2615.
Commune

Town/city

Street

Street number

Additional address component

This section provides information on the Applicant(s), whether a natural person, a legal person governed by private law or a legal person governed by public law.

Where the Applicant is a natural person

In this case, the section 'Person with signing authority for the entity' is not displayed, as the Applicant is the person authorised to sign the Application for Re-Use of Data.

The information relating to the Applicant submitting the Application for Re-Use of Data is pre-filled on the basis of information in the MyGuichet.lu certified business eSpace.

The pre-filled data cannot be changed in the Application for re-use of data. If the pre-filled data is incorrect, the Applicant must update it in the MyGuichet.lu business eSpace by submitting a new Application for Certification.

When several Applicants submit an Application for Re-Use of Data for a common project

In this case, the person designated as the contact person must provide the information relating to each of the participating Applicants. The information input by the contact person must match the information in each Applicant's certified business eSpace. The nature of the link between the Applicant must also be explained in the joint Application for Re-Use of Data.

The processing of *Personal Data* within the SPE

In this case, the following factors must be taken into account:

- the Applicant will qualify as the controller under Article 4 of the GDPR for processing activities carried out within the SPE,
- where several Applicants jointly submit an Application for Re-use of Data, those Applicants will be considered joint controllers under Article 26 of the GDPR. In such cases, the Applicants must enter into an arrangement setting out, in a transparent manner, their respective responsibilities for compliance with GDPR obligations (for example: drafting and providing the data protection notice, determining responsibility for notifying the CNPD in the event of a personal data breach, or carrying out a Data Protection Impact Assessment, where applicable).

For more information on the obligations of controllers, including joint controllers, please see:

https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_fr

5.4 Data Holder(s) of the PSB Data

Steps filling	Data Holder 1
Information ✓	The CGSD (and its subcontractors) may contact the Data Holder(s) when the data is made available or for any additional Information.
Contact person ✓	You may enter up to 10 public sector bodies.
Applicant(s) ✓	
Data Holder 1	Add a public sector body
Description of the context of access to and re-use of data	
Description of data categories	
Appropriate Measures	
Data use and retention periods	
Data users	
Secure processing environment	

Information about the public sector body
Official name *

Official address
Country

Luxembourg

Postcode *

Example: for L-2615, enter 2615.
☐ The address could not be found in the list

The following information must be completed in consultation with the Data Holder.

Public sector body contact information (See Data Catalogue)
First name(s)

Surname

Professional email address *

Please do not enter a private email address
Professional phone number * 

Please do not enter a private phone number

To add other Data Holders, go to the start of the page.

In this section, the Applicant must indicate the information relating to the Data Holder(s). This information may be found in the Catalogue.

The Data Holder agrees to the access to and re-use of the PSB Data it holds [by signing the Application for Re-Use of Data](#). Your Application for Re-Use of Data can only be processed after the Data Holder has signed it.

5.5 Description of the context of access to and re-use of data

5.5.1 Context of your Application for Re-Use of Data

Steps filling	Description of the context of access to and re-use of data
Information ✓	Context Description of the context of your application for access to and re-use of data * 0/3500
Contact person ✓	
Applicant(s) ✓	
Data Holder 1 ✓	
Description of the context of access to and re-use of data	
Description of data categories	

In this field, state the reasons for applying for re-use of public sector data. This enables the CGSD to understand the context of your Application for Re-Use of Data in order to facilitate its processing.

5.5.2 Objectives of your Application for Re-Use of Data

Appropriate Measures	Objectives of the access to and re-use of data * 0/3500
Data use and retention periods	
Data users	
Secure processing environment	

In this field, indicate the specific objectives pursued. These objectives must be related to [the purposes indicated in the Application for Re-Use of Data](#).

5.5.3 Purposes

Select the box(es) corresponding to the purpose(s) pursued by the Applicant(s) *	
☐	Statistical analysis
☐	Education, training or teaching activities (including vocational and higher education)
☐	Scientific research
☒	Historical research
☐	Assessment of Luxembourgish and European public policies
Detailed description of the purpose(s) you have selected above. * 0/3500	

Your Application for Re-Use of Data must pursue one or more of the purposes provided for by the Law, namely:

- statistical analysis;
- education, training or teaching activities (including vocational or higher education);
- scientific research;

- historical research; or
- the evaluation of Luxembourgish or European public policies.

Check the box(es) corresponding to the purpose(s) pursued by the Application for Re-Use of Data. To enable the CGSD to analyse your Application for Re-Use of Data as effectively as possible, we recommend that you carefully identify all the purposes pursued by your Application for Re-Use of Data and ensure that they correspond to the processing you intend to carry out.

Please note that if your Application for Re-Use of Data involves the processing of Personal Data, you must also ensure compliance with the principle of purpose limitation.¹⁰ Under this principle, Personal Data must be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.

Furthermore where the Personal Data is processed for scientific or historical research purposes or statistical purposes, you must also take into account Article [89\(1\) of the GDPR](#) and Articles [63 to 65 of the Law of August 2018 on the organisation of the National Commission for Data Protection and the General Data Protection Regime](#).

5.5.3.1 Statistical analysis

This purpose could be chosen if you plan to produce statistics.

Examples:

- *analyse energy consumption trends by region;*
- *produce annual statistics on the employment rate by sector;*
- *study the distribution of modes of transport used in urban areas.*

5.5.3.2 Education, training or teaching activities

This purpose could be chosen if the purpose of the Application for Re-Use of Data is to:

- develop teaching materials or training for professionals or students, or
- create anonymised case studies for use in academic or professional programmes.

Examples:

- *create anonymised case studies for courses in law or economics;*
- *develop simulated scenarios to train crisis management officers;*
- *Develop interactive modules for learning trade negotiation techniques.*

5.5.3.3 Scientific research¹¹

The concept of 'scientific research' should be understood in a broad manner, encompassing all academic research, including, for example, the social sciences, the humanities and the arts, as well as research with a commercial objective, technological development and innovation.

This purpose could be chosen if, for example, you intend to carry out research activities within the framework of:

¹⁰ V. Article 5(1)(b) of the GDPR.

¹¹ GDPR, recital 159.

- *technological development and demonstration;*
- *innovation activities such as training of AI algorithms, as well as the evaluation and further development of existing algorithms and products for such purposes;¹²*
- *basic research, i.e. theoretical or experimental work, undertaken principally with a view to acquiring new knowledge concerning the fundamental principles of observable phenomena or facts, and not essentially directed towards a practical aim or objective;*
- *applied research, consisting of original work undertaken with a view to acquiring new knowledge. However, it is mainly directed towards a specific practical aim or objective;¹³*
- *research financed by the private or public sector;*
- *studies carried out in the public interest in the field of public health.*

5.5.3.4 Historical research¹⁴

This purpose could be chosen if you intend to produce academic or scientific work on historical periods, or to understand historical trends or facts, without intending to identify individuals.

Examples:

- *study old demographic data to understand the impact of epidemics on the population;*
- *analyse historical data to understand the evolution of migration;*
- *exploit social archives to trace the history of trade union or political movements.*

If you wish to process data for historical research purposes, please note that the GDPR does not apply to deceased persons.

5.5.3.5 Evaluation of Luxembourgish or European public policies

This purpose covers the evaluation of public policies of the State or the European Union:

Examples:

- *the impact of sustainable mobility policies on reducing ₂ CO emissions;*
- *the effects of European vocational training programmes on youth employment;*
- *the effectiveness of public support for innovation for SMEs in Luxembourg;*
- *study of the impact of public policies on the reduction of social inequalities;*
- *the distribution of EU funds in the regions and their influence on economic development.*

5.5.3.6 Detailed description of the purposes you have ticked

Once the purpose(s) have been selected, provide a detailed description of the purpose(s) pursued. Vague, generic or ambiguous explanations should be avoided.

Your description must be sufficiently precise to enable the CGSD to analyse your Application for Re-Use of Data.

¹² EHDS, recital 61.

¹³ Article 1(4) of the amended Law of 3 December 2014 on the organisation of public research centres

¹⁴ GDPR, recital 160.

This description will also be used by the CGSD to analyse application for results exports you want to export are consistent with the purpose(s) you ticked.

5.5.4 Justification of the proportionality of the Application for Re-Use of Data

Justification of the proportionality of the application *	0/3500

Explain here how the envisaged processing activities achieve the legitimate objectives pursued, while remaining limited to what is strictly necessary and appropriate.

This includes showing that the expected benefits of these activities outweigh any negative impacts they may have on Data Subjects, Data Holders and/or third parties.

Your description must enable the CGSD to understand and assess the balance between the objective pursued and the possible infringements of the rights and freedoms of others, taking into account the context in which the processing activities are carried out.

5.6 Description of data categories

Steps filling <table> <tr><td>Information</td><td>✓</td></tr> <tr><td>Contact person</td><td>✓</td></tr> <tr><td>Applicant(s)</td><td>✓</td></tr> <tr><td>Data Holder 1</td><td>✓</td></tr> <tr><td>Description of the context of access to and re-use of data</td><td>✓</td></tr> <tr><td>Description of data categories</td><td></td></tr> <tr><td>Appropriate Measures</td><td></td></tr> <tr><td>Data use and retention periods</td><td></td></tr> </table>	Information	✓	Contact person	✓	Applicant(s)	✓	Data Holder 1	✓	Description of the context of access to and re-use of data	✓	Description of data categories		Appropriate Measures		Data use and retention periods		Description of data categories A detailed description of the data requested must be provided and attached to the procedure. The template is available by clicking on this link. It is an integral part of this application. General information about the data requested The data requested is protected pursuant to Article 3(1) of Regulation (EU) 2022/868 (DGA) for the following reasons: * ☐ the protection of personal data ☐ the protection of intellectual property rights of third parties ☐ commercial confidentiality, including business, professional and company secrets ☐ statistical confidentiality
Information	✓																
Contact person	✓																
Applicant(s)	✓																
Data Holder 1	✓																
Description of the context of access to and re-use of data	✓																
Description of data categories																	
Appropriate Measures																	
Data use and retention periods																	

In this section, specify the categories of data covered by your Application for Re-Use of Data, the grounds for protection applying to the PSB Data and the format in which you wish to receive the data in the SPE.

Please note: the '[Data Description](#)' table must be completed in full and attached to your Application for Re-Use of Data (the template can be downloaded [here](#)), this annex being an integral part of the Application for Re-Use of Data.

5.6.1 The grounds for protection of PSB Data

In this section you must indicate all the [grounds for protection](#) that apply to the PSB Data.

To help you fill in this field, you can reproduce the grounds for protection of PSB Data indicated in the Catalogue, where available.

5.6.2 Special categories of Personal Data

If you request Personal Data, you must indicate whether your Application for Re-Use of Data concerns [special categories of Personal Data](#) within the meaning of Article 9 of the GDPR.

Steps filling	Description of data categories
Information ✓	A detailed description of the data requested must be provided and attached to the procedure. The template is available by clicking on this link . It is an integral part of this application.
Contact person ✓	
Applicant(s) ✓	
Data Holder 1 ✓	
Description of the context of access to and re-use of data ✓	
Description of data categories	General information about the data requested
Appropriate Measures	The data requested is protected pursuant to Article 3(1) of Regulation (EU) 2022/868 (DGA) for the following reasons: *
Data use and retention periods	☒ the protection of personal data
Data users	☐ the protection of intellectual property rights of third parties
Secure processing environment	☐ commercial confidentiality, including business, professional and company secrets
	☐ statistical confidentiality
	Does the application concern special categories of personal data pursuant to Article 9 of Regulation (EU) 2016/679 (GDPR)? *
	☒ Yes
	☐ No

5.6.3 External Data

In addition to PSB Data, you can also request the inclusion of External Data in the SPE.

Would you like to request the integration of data that does not originate from a Luxembourg public sector body? *
☐ Yes
☐ No

Attention: Only answer 'yes', if you want to include data that is not PSB Data in the SPE!

To request the use and inclusion of External Data in the SPE, you must:

- have all necessary rights (e.g. intellectual property rights, commercial confidentiality) for the intended uses,
- comply with legal obligations, in particular those of the GDPR.

☐ The Applicant(s) confirm(s) that they hold all necessary rights to use the data in the context of access to and re-use of * data and, where applicable, that any envisaged processing of personal data complies with the requirements of Regulation (EU) 2016/679 (GDPR).
--

No datasets should be transmitted to the CGSD at this stage.

5.6.4 Data format

Indicate the format in which you request the data to be made available in the SPE. Data can be made available in an anonymised or a pseudonymised format.

In which format do you want to access the data in the secure processing environment? *
☐ In a pseudonymised format
☐ In an anonymised format

For more information on the difference between anonymised data and pseudonymised Personal Data, see [Section 3.2.1](#).

5.6.5 Detailed description of the necessity and proportionality of the requested data

Detailed description of the necessity and proportionality of the data requested. *	0/3500

In this field, explain why the data, as described in the Data Description, and [the format chosen](#) (anonymised or pseudonymised) are necessary in light of all elements of the Application for Re-Use of Data, referencing the context, the objectives, the purposes, the DPIA and the Appropriate Measures Plan.

You must demonstrate that the data to be made available in the SPE is:

- adequate, i.e. appropriate for the intended purpose,
- relevant, i.e. directly related to the intended purpose, and
- limited to what is necessary, thus not going beyond what is required and strikes a balance between the expected benefits and the impact on the rights and freedoms of data subjects.

If you request that the data be made available in the SPE in a pseudonymised format, you must provide a clear and detailed justification of why this format is necessary and why anonymised data would not allow you to achieve your objective.

To assist you in completing this section, the following questions may help guide your response:

- How do processing activities aim to achieve the intended objective?
- Is the data processing proportionate? Do the expected benefits justify the impact on privacy?
- Is all the data covered by the Application for Re-Use of Data necessary and directly related to the intended purpose?

5.6.6 Annex: "Data Description"

- ☐ The Applicant(s) confirm(s) that they have provided comprehensive information on all data covered by the application in the 'Data description' table attached to the application.

The "Data Description" Annex (XLS format) forms an integral part of the Application for Re-Use of Data. You must provide information on all datasets covered by the Application for Re-Use of Data and that you request be made available in the SPE.

The Data Description consists of three types of sheets: Target Data, PSB Data and External Data.

For PSB Data and External Data, use within a sheet for each dataset that is the subject of your Application for Re-Use of Data and number it according to the template (PSB Data 01, PSB Data 2, External Data 01, ...).

1. On the '**Target Data**' sheet, describe the data that you request be made available in the SPE after the application of the Appropriate Measures. This sheet must also provide an inventory of the PSB and External Data sheets.

2. One or more sheets describing the **PSB Data**: on this sheet, describe the PSB Data, as it exists prior to the application of the Appropriate Measures. Please complete these sheets with the Data Holder(s).
3. One or more sheets describing the **External Data**: on this sheet, describe the External Dataset as it exists prior to the application of the Appropriate Measures.

5.6.6.1 Target Data Sheet

5.6.6.1.1 Categories of Data Subjects in the requested Target Data

Categories of data subjects				
<i>The Applicant shall describe all categories of data subjects concerned by the datasets to be entered into the SPE.</i>				
Category	Description	Vulnerable subjects?	Size of the group*	Justification for the necessity of processing****

If Personal Data is processed, indicate all categories of Data Subjects in this section (e.g. Luxembourg homeowner, jobseeker with residence in Luxembourg, etc.).

For each category of Data Subjects, you must provide a description of the category, indicating whether vulnerable persons are involved, the size of the group and the justification for the necessity of the processing.

Vulnerable persons are persons who, because of their age, capacity or situation, are considered to be in need of greater protection, such as minors or persons under guardianship.

The size of the group corresponds to the number of Data Subjects in relation to the general population, either accurately or by an estimate.

5.6.6.1.2 Geographical and temporal coverage of the requested Target Data

Geographical coverage of the data to be made available <i>The Applicant shall describe the geographical coverage of the dataset to be entered into the SPE.</i>
Text (3,500)
Temporal coverage of the data to be made available <i>The Applicant shall describe the temporal coverage of the dataset to be entered into the SPE.</i>
Text (3,500)

This section aims to ensure that the Target Data requested to be made available in the SPE is limited to what is strictly necessary.

For example, do not request data for the whole of Luxembourg if your project only aims to assess the impact of a pilot programme in a few municipalities.

Similarly, use time ranges rather than exact time points, e.g. the month of an event instead of the exact date and do not request monthly data from 2010 to the present, if the project only aims to evaluate a policy introduced in 2022.

5.6.6.1.3 Categories of Target Data to be entered in the SPE

Categories of data to be entered into the SPE						
The Applicant shall describe all categories of data to be made available in the SPE.						
Category	Description	Grounds for protection	Description of the grounds for protection*	Category of data subjects directly concerned by the data category**	Category of data subjects indirectly concerned by the data***	Details regarding the necessity of processing****

* In case "multiple protection grounds" indicated in "Ground for protection"

** In case of personal data, the data subjects directly concerned by the data: for example, for the name of the doctor in a consultation, the data subject concerned is the doctor.

*** In case of personal data, the data subjects indirectly concerned by the data: for example, for the name of the doctor in a consultation, the data subject indirectly concerned is the patient.

**** The Applicant shall justify that the processing of this category of data is necessary for the purpose pursued.

In the 'Category' column, indicate the category of Target Data you request be made available in the SPE (e.g. data reference period, pseudonymised identifier, country of residence, etc.) and provide, if necessary, a **description of the category**.

Categories of data to be entered into the SPE						
The Applicant shall describe all categories of data to be made available in the SPE.						
Category	Description	Grounds for protection	Description of the grounds for protection*	Category of data subjects directly concerned by the data category**	Category of data subjects indirectly concerned by the data***	Details regarding
			Personal data in the context of the GDPR Commercial confidentiality, including business, professional and company secrets Statistical confidentiality Intellectual property rights of third parties Multiple grounds for protection Unprotected			

* In case "multiple protection grounds" indicated in "Ground for protection"

** In case of personal data, the data subjects directly concerned by the data: for example, for the name of the doctor in a consultation, the data subject concerned is the doctor.

*** In case of personal data, the data subjects indirectly concerned by the data: for example, for the name of the doctor in a consultation, the data subject indirectly concerned is the patient.

**** The Applicant shall justify that the processing of this category of data is necessary for the purpose pursued.

For each category requested, choose (from the drop-down menu) **the ground(s) for protection ground(s)** apply to that category. If "multiple grounds of protection" is selected, enter all applicable grounds in the "Description of grounds of protection" column.

Categories of data to be entered into the SPE						
The Applicant shall describe all categories of data to be made available in the SPE.						
Category	Description	Grounds for protection	Description of the grounds for protection*	Category of data subjects directly concerned by the data category**	Category of data subjects indirectly concerned by the data***	Details regarding the necessity of processing****

* In case "multiple protection grounds" indicated in "Ground for protection"

** In case of personal data, the data subjects directly concerned by the data: for example, for the name of the doctor in a consultation, the data subject concerned is the doctor.

*** In case of personal data, the data subjects indirectly concerned by the data: for example, for the name of the doctor in a consultation, the data subject indirectly concerned is the patient.

**** The Applicant shall justify that the processing of this category of data is necessary for the purpose pursued.

If the Target Data requested constitutes Personal Data, choose from the drop-down menu **the categories of Data Subjects**, which have been previously identified in the "[Categories of Data Subjects](#)" section (see section 5.6.6.1.1).

Categories of data to be entered into the SPE						
The Applicant shall describe all categories of data to be made available in the SPE.						
Category	Description	Grounds for protection	Description of the grounds for protection*	Category of data subjects directly concerned by the data category**	Category of data subjects indirectly concerned by the data***	Details regarding the necessity of processing****

* In case "multiple protection grounds" indicated in "Ground for protection"

** In case of personal data, the data subjects directly concerned by the data: for example, for the name of the doctor in a consultation, the data subject concerned is the doctor.

*** In case of personal data, the data subjects indirectly concerned by the data: for example, for the name of the doctor in a consultation, the data subject indirectly concerned is the patient.

**** The Applicant shall justify that the processing of this category of data is necessary for the purpose pursued.

For each category of Target Data for which provision in the SPE is requested, **justify** why this category is necessary to carry out your project.

5.6.6.1.4 Frequency at which the data should be made available

Regular data provision	
In case the datasets are to be made available on a recurring basis, specify the frequency of provision	
Frequency of provision	Once
	Once
	Annual

If you require the data to be made available on a recurrent basis, specify the requested frequency. You can choose between one-off or periodic data extraction (e.g. annual).

5.6.6.1.5 Target Data Dictionary

Data dictionary relating to the data to be entered into the SPE			
Number of datasets to be made available			
Dataset format		CSV	
Detailed list of variables			
Variable code	Description	Format	Data category

Indicate the number of Target Datasets you request be integrated into the SPE and their format (e.g. CSV format).

You also need to provide a dictionary for the Target Dataset that you want to see embedded in the SPE. This dictionary must include, for each variable, the corresponding code, description, format and Target Data category. The same category of Target Data can be represented by multiple data variables (e.g. address information can be spread across multiple columns in a tabular dataset).

5.6.6.1.6 Inventory of PSB and External Data Sheets

Inventory of data sheets			
List of datasets to be collected from PSBs			
Sheet	Dataset name	PSB Data Holder	Catalogue ID
PSB Data 01			
PSB Data 02			

List of external datasets held by the Applicant	
Sheet	Dataset name

In the “**Sheet**” column, list all the sheets that are used.

In the “**Dataset name**” column, indicate:

- for PSB Data, the name of the dataset as it appears in the Catalogue or has been communicated to you by the Data Holder,
- for External Data, the name of the dataset, as it appears on the [Open Data Portal](#) or that you have assigned to the dataset (where the data is provided by the Applicant).

The name indicated in the column “Dataset name” will be automatically included in the title of each corresponding sheet.

In the “**PSB Data Holder**” column, indicate the official name of the Data Holder. If applicable, use the name found in the “Publisher” section of the [Catalogue](#).

In the “**Catalogue identifier**” column, indicate, where applicable, the identifier of the PSB Dataset entered in the [Catalogue](#) or of the open dataset entered on the [Open Data Portal](#).

WORK ABSENCES

☐ Description
 ☐ General information
 ☐ Access conditions
 ☐ Temporal coverage
 ☐ Data Dictionary
 ☐ Export

Description

This dataset contains all recorded periods of absence for private status employees. This dataset is part of those provided by the IGSS within the framework of the Luxembourg Microdata Platform on Labour and Social Protection. All datasets offered by the IGSS are designed to be interoperable through the use of common pseudonymized identifiers, enabling the linkage of information across different datasets. All the variables in this dataset are personal data and are subject to GDPR compliant protection measures. Scope: absence periods carried out by private status employees. Delay for providing the most recent data: current month -3. Data sources : CCSS.

Publisher **Inspection générale de la sécurité sociale (IGSS)**

Identifier **1e772270-caac-11f0-a122-8aadbbc611c1**

Contact point [Microdata platform](#)

5.6.6.2 Sheets for PSB Data

5.6.6.2.1 Conditions and costs for making PSB Data available

0				
Conditions of data availability				
Specify whether the Data Holder has set specific conditions for making the data available. To identify these conditions, the Applicant shall refer to the conditions for data access as defined in the public sector data catalogue or obtain them from the Data Holders.				
Explain how the conditions will be indeed respected during data use in the SPE and in the planned exports of results.				
Texte (3 500)				

Where applicable, indicate the conditions defined by the Data Holder for the provision of each set of PSB Data. You can refer to the access conditions described in the Catalogue or obtain this information directly from the Data Holders.

In addition, specify how these conditions will be respected when using the PSB Data, as well as when creating and exporting the results.

5.6.6.2.2 Geographical and temporal coverage of the PSB Data

Geographical coverage of the data				
Specify the coverage of the data made available by the Data Holder.				
Temporal coverage of the data				
Specify the coverage of the data made available by the Data Holder.				
Text (3,500)				

Specify the geographical and temporal coverage of the PSB Data you request be made available by the Data Holder. The purpose of this description is to enable the CGSD to analyse the need for the PSB Data requested and to delimit the PSB Data that must be provided by the Data Holder in the event of authorisation.

5.6.6.2.3 Categories of Data Subjects in the PSB Data

Categories of data subjects concerned by the dataset					
The Applicant shall describe all categories of data subjects concerned by the data held by the Data Holder, specifying whether it is requested to use these categories in the SPE.					
Name of category	Description	Vulnerable subjects?	data	Usage in SPE	List of operations applied to ensure the reduction of coverage of the data subject in the target dataset.

From the information provided by the Data Holder, list all categories of Data Subjects included in the PSB Data, irrespective of whether you intend to request that the categories be made available.

For each category of Data Subjects, you must:

- indicate whether you request that this category be made available in the SPE,
- explain how you propose limiting the scale of the PSB Data to those that are strictly necessary for the Application for Re-Use of Data.

5.6.6.2.4 Categories of PSB Data

Categories of data concerned by the dataset						
<i>The Applicant shall describe all data categories present in the data held by the Data Holder, specifying whether the identified data category is requested for use in the SPE. For each data category for which the Data Holder identifies a use risk, the Applicant shall indicate whether the data category is requested to be used in the SPE and provide references to the associated protection measures.</i>						
Name of category	Ground for protection	Description of the ground for protection*	Category of data subjects directly concerned**	Category of data subjects indirectly concerned***	Risk identified by the Data Holder	Usage

Describe all categories of PSB Data present in the PSB dataset. For each of them, specify whether you request the data should be included in the Target Data made available in the SPE. For each category identified, collect the following information from the Data Holder:

- the categories of Data Subjects,
- the grounds of protection applicable to the PSB Data,
- the classification of the risk of re-identification and a description of the risks associated with the use of this category of PSB Data.

In the [Appropriate Measures Plan](#), describe the associated preparation to be carried out for each category of PSB Data that you request.

5.6.6.2.5 Description of the format and volume of the PSB Dataset

Description of the dataset	
Format of the dataset?	
Number of records in the dataset?	
Total size of the dataset (in Mb)?	
Will the Data Holder minimise variables that are not necessary for the applicant before making the data available to the CGSD?	
Does the Data Holder wish to encrypt certain variables before making the data available to the CGSD?	

From the Data Holder, obtain information about the format in which the requested PSB Data will be provided. The default format for tabular data is “CSV”. In this section, you should also provide an estimate of the number of records and the approximate size of the file in megabytes.

The PSB Data may be prepared by the Data Holder before being sent to the CGSD. This preparation may include the minimisation of certain variables or the application of encryption measures. Any such preparation must be clearly indicated.

5.6.6.2.6 PSB Data Dictionary

Provide a dictionary for the PSB Dataset. Use the same level of granularity used for Target Data.

5.6.6.3 Sheets for External Data

5.6.6.3.1 Conditions for making the External Data available

Description of the use of External Data				
0				
Conditions of data availability				
<i>Specify whether specific conditions of data availability apply to the data</i>				
Text (3,500)				
<i>Explain how the conditions will be indeed respected during data use in the SPE and in the planned exports of results.</i>				
Text (3,500)				

Where applicable, indicate the conditions defined by the holder of the External Data for the provision of each set of External Data. In addition, specify which measures will be put in place to comply with these conditions.

5.6.6.3.2 External Data Pseudonymisation Measures

Pseudonymisation measures at the source				
<i>Specify whether data pseudonymisation at the source is used and list the personal identifiers concerned by this pseudonymisation</i>				
Text (3,500)				

Specify whether the External Data will be provided in a pseudonymised format and, if so, which direct identifiers have been pseudonymised.

5.6.6.3.3 Geographical and temporal coverage of the External Data

Geographical coverage of the data				
<i>Specify the coverage of the data made available.</i>				
Text (3,500)				
Temporal coverage of the data				
<i>Specify the coverage of the data made available.</i>				
Text (3,500)				

Describe the geographical and temporal coverage of the External Data for which you request the inclusion in the SPE. The description must enable the CGSD to understand how the External Data could, if applicable, be combined with the PSB Data.

5.6.6.3.4 Categories of Data Subjects in the External Data

Categories of data subjects concerned by the dataset				
<i>The Applicant shall describe all categories of data subjects concerned by the data, whether or not they are used in the SPE.</i>				
Name of category	Description	Vulnerable data subjects?	Usage in SPE	Reduction of scale

List all categories of Data Subjects included in the External Dataset and explain how you propose to limit the External Data to that strictly necessary for the Application for Re-Use of Data. Use the same level of granularity as used for PSB Data.

5.6.6.3.5 Categories of data in the External Dataset

Categories of data covered by the dataset						
<i>The Applicant shall describe all data categories present in the data, whether or not they are used in the SPE. For each data category with an identified use risk, the Applicant shall indicate whether the data category is requested to be used in the SPE and provide references to the associated protection measures.</i>						
Name of category	Ground for protection	Category of data subjects*	Description of the ground for protection	Risk classification	Description of the risk	Usage

In this section, describe all categories of data present in the External Data. Use the same level of granularity as used for PSB Data.

5.6.6.3.6 Description of the format and volume of the External Data

Indicate the format and size of the dataset, including the number of records and the size of the file in megabytes.

Description of the dataset	
Format of the dataset?	
Number of records in the dataset?	
Total size of the dataset (in Mb)?	

5.6.6.3.7 External Data Dictionary

Data dictionary relating to the data to be entered into the SPE			
<i>Detailed list of variables</i>			
Variable	Description	Format	Data category

Provide a dictionary for the External Dataset. Use the same level of granularity as used for PSB Data.

5.6.6.4 Resources and final checklist

- ☐ Complete the Excel file called "[Data Description](#)".
- ☐ If necessary, ask the LNDS for help by [contacting its helpdesk](#)
- ☐ Complete the "PSB Data" sheet(s) in collaboration with the Data Holder(s).
- ☐ If applicable, complete the "External Data" sheet(s).
- ☐ Complete the Target Data sheet to define the data you want to access in the SPE after the CGSD has applied the Appropriate Measures.
- ☐ Ensure that justification for needing the "Target Data" is clear and duly substantiated.
- ☐ Check the consistency of the references between the categories of Data Subjects, the categories of Target Data, PSB Data and, where applicable, External Data, as well as the corresponding variable tables.
- ☐ Verify that the data variable codes in the data dictionary segments correspond to those indicated in the Appropriate Measures Plan, in particular in the section detailing the preparation required before the Target Data is made available in the SPE.
- ☐ Check the consistency of the categories of Target Data, PSB Data and, where applicable, External Data with those mentioned in the Appropriate Measures Plan, in particular in the section relating to the assessment of re-identification risks.

5.7 Lawfulness

The section on lawfulness is shown and must be filled in when you request access to data [in a pseudonymised format in the SPE](#). The lawful condition for processing of Personal Data is the basis that enables a controller to use the Personal Data. Without a lawful condition for processing, the processing is considered illegal. This field is obligatory.

If your processing of Personal Data serves several purposes, you must define a legal basis for each of them and check the boxes corresponding to the appropriate legal bases.

Where the processing of Personal Data concerns [special categories of Personal Data](#), it must be based both on one of the lawful conditions for processing laid down in Article 6 of the GDPR and on one of the legal bases of Article 9(2) of the GDPR.

5.7.1 Lawful conditions for processing under Article 6 of the GDPR

Application for re-use of data (Data Factory)

Steps filling	Lawfulness
Information	✓
Contact person	✓
Applicant(s)	✓
Data Holder 1	✓
Description of the context of access to and re-use of data	✓
Description of data categories	✓
Lawfulness	

Lawfulness

Lawfulness of the access to and re-use of data

Select the legal basis or bases pursuant to Article 6 of Regulation (EU) 2016/679 (GDPR) justifying the processing of personal data. *

- ☐ Consent of the data subject (Art. 6.1, a) of the GDPR)
- ☐ Performance of a contract concluded with the data subject (Art. 6.1, b) of the GDPR)
- ☐ Compliance with a legal obligation to which the Applicant(s) is(are) subject (Art. 6.1, c) of the GDPR)
- ☐ The vital interests of the data subject or another natural person (Art. 6.1, d) of the GDPR)
- ☐ The performance of a task carried out in the public interest by the Applicant(s) (Art. 6.1, e) of the GDPR)
- ☐ The legitimate interests pursued by the Applicant(s) or a third party (Art. 6.1, f) of the GDPR)

5.7.1.1 The consent of the Data Subject (Article 6.1(a) of the GDPR)

The Personal Data of a Data Subject may be processed with his or her consent.

To be valid, consent must be:

- ⇒ “free”: the Data Subject must have a genuine choice and be able to refuse or withdraw consent without suffering significant negative consequences. Consequently, consent will not be given freely if the Data Subject is unable to refuse or withdraw consent at any time;
- ⇒ “specific”: consent must be given for each processing activity and for a specific purpose. In case of multiple purposes, the Data Subject must be able to give his or her consent independently of one or other of those purposes;
- ⇒ “informed”: the Data Subject must understand what data is processed, why and how and must therefore receive a certain amount of information concerning the data use before consenting;
- ⇒ “unambiguous”: consent must be given unambiguously by a clear statement or other positive act. By way of example, consent cannot be inferred from the silence of the Data Subject.

These four criteria are cumulative and must be met in order for the consent of the Data Subject to be valid.

For more information on the consent of the Data Subject, see:

- [EDPB Guidelines 05/2020 on consent within the meaning of Regulation \(EU\) 2016/679](#)

5.7.1.2 The performance of a contract to which the data subject is party (Article 6.1(b) of the GDPR)

Personal Data may also be processed when the envisaged processing is necessary for the performance of a valid contract to which the Data Subject is party, or in order to take steps at the request of the Data Subject prior to entering into a contract.

Please note that this lawful condition for processing only applies where the processing activities are objectively necessary for the performance of the contract or the pre-contractual measures requested by the Data Subject. It cannot justify processing activities which pursue other purposes, in particular commercial purposes, of the controller, where they are not essential for the performance of the contract or the pre-contractual measures requested.

For more information on this lawful condition for processing, see:

- [EDPB Guidelines 2/2019 on the processing of personal data under Article 6\(1\)\(b\) of the GDPR in the context of the provision of online services to data subjects](#)

5.7.1.3 Compliance with a legal obligation (Art. 6.1(c) of the GDPR)

In order to constitute a valid lawful condition for processing, the legal obligation must fulfil the following conditions:

- it must be set out by Luxembourg or European Union law to which the controller is subject;
- it must be binding on the controller, i.e. the controller must comply with it and have no discretion as to whether or not to proceed with the processing.

An Authorisation is not necessary for any legal obligations applicable to a controller would be subject, such as:

- *an administration, which publishes official employment statistics in accordance with its organic law.*
- *an undertaking, which keeps documents on the basis of a legal obligation.*
- *an authority, which collects data to produce reports required by EU legislation.*

5.7.1.4 Vital interests of the data subject or another natural person (Art. 6.1(d) of the GDPR)

The processing of Personal Data may be necessary to protect a person's life or health. That lawful condition for processing is to be interpreted strictly and may be used only where it is impossible to have recourse to another lawful condition for processing. This basis may be used in exceptional and urgent situations, for example, in the event of a threat to the person's life or where the person is unable to express his or her consent.

5.7.1.5 The task carried out in the public interest or in the exercise of official authority (Article 6.1(e) of the GDPR)

This lawful condition for processing allows for processing of Personal Data where the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Public administrations, ministries, municipalities, and other public sector bodies may rely on this legal basis for processing carried out in the context of their public service tasks.

Processing of personal data may be based on this lawful condition for processing where the purpose pursued corresponds to a task assigned to one of the aforementioned public bodies under the applicable legal framework, and where the processing is necessary to achieve that purpose.

5.7.1.6 The legitimate interests of the controller or a third party (Article 6.1(f) of the GDPR)

Where the controller intends to rely on this lawful condition for processing, three cumulative conditions must be met:

- the interest must be legitimate: the interest must be (i) lawful, (ii) clearly and precisely articulated, and (iii) real and present and no speculative:
 - o the controller should therefore identify the legitimate interest in detail;
- the processing must be necessary: the envisaged processing of the data must make it possible to achieve the objective pursued. In addition, the controller must assess whether the purposes can reasonably be achieved just as effectively by other means less restrictive of the fundamental rights and freedoms of data subjects.
 - o the controller must ensure that there are no alternative, less intrusive, just as effective, means;
- a balancing exercise of the opposing rights and interests at issue: a balancing test must be carried out to ensure that the interests or fundamental rights and freedoms of the Data Subjects do not override the legitimate interests pursued by the controller:
 - o the controller must perform this balancing test and the analysis must be attached to the Application for Re-Use of Data.

Public authorities acting in the performance of their tasks cannot base their processing activities on this lawful condition for processing.

For more information on this lawful condition for processing, see:

- [EDPS Guidelines 1/2024 on the processing of Personal Data based on Article 6\(1\)\(f\) of the GDPR \(version published for public consultation\)](#)
- [Opinion 06/2014 of the Article 29 Working Party on the concept of legitimate interest pursued by the data controller within the meaning of Article 7 of Directive 95/46/EC \(WP217\)](#)

5.7.2 Special categories of personal data pursuant to Article 9 of the GDPR

Select the legal basis or bases pursuant to Article 9 of Regulation (EU) 2016/679 (GDPR) justifying the processing of special categories of personal data. *

- ☐ The explicit consent of the data subject (Art. 9.2, a) of the GDPR)
- ☐ Carrying out the obligations and exercising the specific rights of the Applicant(s) in the field of employment and social security and social protection law (Art. 9.2, b) of the GDPR)
- ☐ Protection of the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent (Art. 9.2, c) of the GDPR)
- ☐ Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim (Art. 9.2, d) of the GDPR)
- ☐ Processing relates to personal data which are manifestly made public by the data subject (Art. 9.2, e) of the GDPR)
- ☐ The establishment, exercise or defence of legal claims (Art. 9.2, f) of the GDPR)
- ☐ Reasons of substantial public interest (Art. 9.2, g) of the GDPR)
- ☐ Preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems (Art. 9.2, h) of the GDPR)
- ☐ Reasons of public interest in the area of public health (Art. 9.2, i) of the GDPR)
- ☐ Archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (Art. 9.2, j) of the GDPR)

If the Application for Re-Use of Data concerns the processing of special categories of Personal Data within the meaning of Article 9(1) of the GDPR, you must check the box(es) corresponding to the legal basis(s) of Article 9(2) of the GDPR.

The processing of special categories of Personal Data within the meaning of Article 9 of the GDPR is prohibited, unless it is based on one of the legal bases of Article 9(2) of the GDPR, in addition to one of the lawful conditions for processing provided for in Article 6 of the GDPR.

5.7.2.1 The explicit consent of the data subject (Art. 9.1(a) of the GDPR)

The processing of special categories of Personal Data may be based on the explicit consent of the Data Subject. However, this exception does not apply where European Union or Luxembourg law provides that the prohibition on processing these special categories of Personal Data cannot be lifted by the Data Subject.

For more information on the collection of the Data Subject's 'explicit' consent, see:

- [EDPS Guidelines 5/2020 on consent within the meaning of Regulation \(EU\) 2016/679](#)

5.7.2.2 Obligations and exercise of rights under labour, social security and social protection law (Art. 9.2(b) of the GDPR)

Special categories of Personal Data can be processed on the basis of this lawful basis if the processing is:

- necessary for the performance of the obligations and the exercise of the controller's or the Data Subject's own rights in relation to employment, social security and social protection law, and
- authorised by European Union or Luxembourg law or by a collective agreement.

5.7.2.3 Safeguarding the vital interests of the data subject or another natural person (Art. 9.2(c) of the GDPR)

This lawful basis may be invoked in exceptional situations and in cases of absolute urgency if the processing is necessary to safeguard the vital interests of the Data Subject or of another natural person, where that person is physically or legally incapable of giving consent.

5.7.2.4 Processing by a foundation, association or other non-profit body (Art. 9.2(d) of the GDPR)

This lawful basis concerns foundations, associations or any other not-for-profit bodies with a political, philosophical, religious or trade union aim.

It may serve as a basis if the controller, in the context of its legitimate activities and subject to appropriate guarantees, carries out processing of Personal Data that relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the Personal Data are not disclosed outside that body without the consent of the Data Subjects.

5.7.2.5 The processing concerns data that are manifestly made public by the data subject (Art. 9.2 (e) of the GDPR)

This lawful basis may only be used if the controller can demonstrate that the Data Subject has explicitly and by a clear affirmative action intended to make his or her Personal Data accessible to the general public.

For more information on the interpretation of this condition, see:

- [Judgment of the Court of Justice of the European Union of 4 October 2024, Case C-446/21 Schrems v Meta, ECLI:EU:C:2024:834](#)

5.7.2.6 The establishment, exercise or defence of legal claims (Art. 9.2(f) of the GDPR)

This lawful basis may be invoked where the processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

5.7.2.7 Reasons of substantial public interest (Art. 9.2(g) of the GDPR)

Special categories of Personal Data can be processed where it is necessary for reasons of substantial public interest, in accordance with European Union or Luxembourg law, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject

This lawful basis may be invoked, for example, where processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters.¹⁵

5.7.2.8 Medicine and health (Art. 9.2 (h) of the GDPR)

Processing may be based on this provision¹⁶ if it satisfies three cumulative conditions.

The first condition requires that the processing be necessary for the purposes of:

¹⁵ Recital 46 of the GDPR.

¹⁶ That provision must be read in conjunction with Article 9(3) of the GDPR.

- preventive or occupational medicine,
- for the assessment of the working capacity of the employee,
- medical diagnosis,
- the provision of health or social care or treatment,
- or the management of health or social care systems and services

The second condition requires that the processing is carried out on the basis of a provision of Luxembourg or European Union law or under a contract concluded with a health professional.

Finally, the third condition relates to the duty of confidentiality to which persons authorised to carry out such processing are bound. Under Article 9(3) of the GDPR, those persons must be subject to an obligation of professional secrecy.¹⁷

For example, this is the case for data processing carried out in the context of the pre-recruitment medical examination carried out by the occupational physician.¹⁸

5.7.2.9 Public interest grounds in the field of public health (Art. 9.2(i) of the GDPR)

Processing may be based on this provision where it is necessary for reasons of public interest in the field of public health, such as:

- protection against serious cross-border threats to health,
- ensuring high standards of quality and safety of healthcare, medicines and medical devices.

Such processing must be carried out on the basis of a provision of Luxembourg or European Union law and provides for appropriate and specific measures to safeguard the rights and freedoms of the Data Subject, in particular professional secrecy.

5.7.2.10 Archival purposes in the public interest, scientific or historical research or statistics (Art. 9.2(j) of the GDPR)

This legal basis may be used where the processing is necessary for archiving purposes in the public interest, for [scientific research](#), [historical research](#) or [statistical purposes](#).

In this case, the processing must be based on a national or European law (such as the Law, read together with the DGA), be proportionate, respect the right to data protection and provide for appropriate and specific measures to protect the fundamental rights and interests of the Data Subject.

¹⁷ Judgment of the Court of Justice of the European Union of 21 December 2023, Case C-667/21 *Krankenversicherung Nordrhein*, ECLI:EU:C:2023:1022, para. 44

¹⁸ Article L.326-1 of the Luxembourg Labour Code.

5.8 Appropriate Measures Plan

Application for re-use of data (Data Factory)

Steps filling
Information ✓
Contact person ✓
Applicant(s) ✓
Data Holder 1 ✓
Description of the context of access to and re-use of data ✓
Description of data categories ✓
Lawfulness ✓
Appropriate Measures
Data use and retention periods
Data users
Rights and freedoms
Secure processing environment

Appropriate Measures

The template of the Appropriate Measures Plan is available [by clicking on this link](#).

Appropriate Measures Plan

The Appropriate Measures Plan attached to this application sets out in detail the appropriate measures that are intended to ensure compliance with the requirements regarding anonymisation, pseudonymisation and aggregation of the data, namely with regard to:

- the technical and operational measures to prevent any re-identification of data subjects.
- the technical and organisational measures necessary to prevent the misuse or unauthorised use of data and to protect the rights and interests of the Data Holder(s) and the data subjects
- the appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

☐ By checking this box, the Applicant(s) declare(s) that the information set out above is included in the Appropriate Measures Plan and acknowledge(s) and accept(s) that the CGSD may impose all measures necessary to safeguard the protected rights and interests (without limitation), the protection of personal data, intellectual property rights, commercial confidentiality, including business, professional and company secrets, statistical confidentiality, rights of third parties, data confidentiality and the proper operation of the secure processing environment.

5.8.1 Purpose of the template

Based on the [template provided](#), you must draw up an Appropriate Measures Plan. The purpose of this document is to describe the Appropriate Measures that you propose be implemented to ensure the protection of the requested data.

The Appropriate Measures set out in this Appropriate Measures Plan must cover the entire life cycle of the data, from its provision by the Data Holder, through its preparation and provision as Target Data in the SPE, to its use within the SPE and the export of the results.

Important: The Appropriate Measure Plan constitutes an integral part of your Application for Re-Use of Data. It serves as the basis for the CGSD to determine the Appropriate Measures to be applied as well as the Target Data that may be made available.

This document is the primary basis for describing the data processing activities that are the subject of the Application for Re-Use of Data, the planned protection measures and the risk management approach under the Law and the DGA. It is essential to ensure that the information contained therein is consistent with the Data Description, as well as with all the information and documents provided in the context of the Application for Re-Use of Data.

The preparation of this document must be carried out in collaboration with the Data Holder.

Important: To help you complete the Appropriate Measures Plan, please refer directly to the annex “Appropriate Measures Plan” (the template can be downloaded [here](#)).

The Appropriate Measures Plan must include, at least:

- the technical and operational measures to prevent any re-identification of the Data Subjects,
- the sufficient technical and organisational measures to prevent any misuse or unauthorised use of Target Data and Work Data and to protect the rights and interests of the Data Holder, third parties and Data Subjects.
- The appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

Attention: In addition to the Appropriate Measures proposed in this document, contracts may be necessary between Data Holders and Applicants for the provision of data protected by intellectual property rights or trade secrets.

5.8.2 Final checklist and resources

- ☐ Download the [template of the Appropriate Measures Plan](#).
- ☐ Consult the [List of processing operations](#).
- ☐ Ensure that you have collected the information necessary to complete the Appropriate Measures Plan, including:
 - information on the activities of the Applicant(s) and any potential conflicts of interest,
 - details of the capacity required for the ETS (operating system, disk type, CPU, memory, storage capacity and number of ETS Users),
 - the needs in terms of Technological Solutions, including the list of programming languages, packages and libraries needed to generate the results,
 - information on the physical sites from which the SPE will be accessed,
 - an initial description of how the results will be generated,
 - information, if any, on the archiving requirements (e.g. whether it will be requested, as well as details on its duration and content).
- ☐ Complete the various sections of the Appropriate Measures Plan.
- ☐ Ensure that the Data Description is finalised, including Target Data, PSB Data and External Data, and that it is consistent with the Appropriate Measures Plan.
- ☐ If necessary, ask the LNDS for help by [contacting its helpdesk](#)
- ☐ For more information on relevant risk assessment concepts, Applicants may also consult:
 - ISO/IEC [27559:2022 on "Privacy enhancing data de-identification frameworks"](#).

5.9 Duration

The Authorisation sets out the Authorised Duration, during which Users will have access to the SPE, as well as, where applicable, the archival period.

Application for re-use of data (Data Factory)

Steps filling

Information ✓

Contact person ✓

Applicant(s) ✓

Data Holder 1 ✓

Description of the context of access to and re-use of data ✓

Description of data categories ✓

Lawfulness ✓

Appropriate Measures ✓

Data use and retention periods

Data users

Rights and freedoms

Secure processing environment

Data use and retention periods

Indication of the data use and retention periods

Duration (in days) of the use of the secure processing environment *

Should the data be archived after having been processed in the secure processing environment? *

☒ Yes

☐ No

Clear identification of items to be archived, with supporting reasons for the request * 0/3500

Duration (in days) of retention period in the archiving system *

Justification that the periods set out above are necessary * 0/3500

5.9.1 Authorised Duration

In the field 'Duration (in days) of use of the secure processing environment', you must enter the duration in days during which you plan to use the SPE. If, while using the SPE, you discover that the Authorised Duration is insufficient, you may request an extension thereof.

5.9.2 Archival period

You can request that the Target Data, Work Data or External Technology Solutions be archived following the processing carried out in the SPE. However, if you did not request archiving of data when submitting your Application for Re-Use of Data, you still have the possibility to request archiving after obtaining the Authorisation.

If you select "Yes", please indicate the intended archival period, expressed in days. You must also specify which items will be archived.

5.9.3 Justification of data use and retention periods

In the final field, provide a justification of the necessity of the requested data use and archival periods in light of the purposes pursued (for example: reproducibility of results, audits, or compliance with research integrity policies, etc.). This justification must demonstrate that the requested durations are limited to what is strictly necessary.

If, during the course of the project, you consider it necessary to provide for archiving or to extend the archival period, you may submit a request to the CGSD.

 LETZDATA

42

5.10 Users

Application for re-use of data (Data Factory)

Steps filling

Information	✓
Contact person	✓
Applicant(s)	✓
Data Holder 1	✓
Description of the context of access to and re-use of data	✓
Description of data categories	✓
Lawfulness	✓
Appropriate Measures	✓
Data use and retention periods	✓
Data users	
Rights and freedoms	

Data users

These are the natural persons who would have access to the secure processing environment. You can include up to 10. The User list must be provided in a table and attached to this procedure. The template is available [by clicking on this link](#).

Users

Maximum number of users *

In this section, indicate the number of Users who would have access to the SPE. You can specify a maximum of 10 Users. You will also need to fill in the "User List".

Attention: the "User List" must be completed and attached to your Application for Re-Use of Data (the template can be downloaded [here](#)), this annex being an integral part of the Application for Re-Use of Data.

Only Users indicated on this list can be authorised to access the SPE. It is therefore essential to indicate them all. You may also request the addition, replacement or removal of a User during the use of the SPE.

How to fill in the User List:

Indicate the reference number of the Application for Re-Use of Data.

Columns B and C: Indicate the first name(s) and surname of the Users.

Columns D and E: Enter the name of the Applicant and describe the link between the User and the Applicant (e.g. employee of the Applicant, collaboration via a subcontract, etc.).

Column F: Enter the User's professional e-mail address

Column G: For each User, specify the country from which that User will access the SPE. Any access to the SPE from a country other than the 27 EU Member States or the three countries of the European Economic Area (EEA), namely Norway, Liechtenstein and Iceland, is considered a data transfer to a third country and must, as such, comply with the requirements of Chapter V of the GDPR.

Column H: Indicate the status of the User (active, add, remove).

For the rules applicable to data transfers to third countries, please refer to the [General Terms and Conditions for the use of the secure IT environment](#).

For more information, you can also consult:

- [The list of third countries with an adequacy decision on the European Commission's website](#)
- [EDPS Guidelines 3/2018 on the territorial scope of the GDPR \(Article 3\)](#)
- [EDPS Guidelines 5/2021 on the interaction between the application of Article 3 and the provisions on international transfers pursuant to Chapter V of the GDPR](#)

5.11 Rights and freedoms

Application for re-use of data (Data Factory)	
Steps filling	Rights and freedoms
Information ✓	Impact analysis and information notice
Contact person ✓	☐ The data protection impact assessment, containing all the information required by Article 35 of Regulation (EU) 2016/679 (GDPR), is attached to the application. *
Applicant(s) ✓	☐ The information notice, which, in line with the principle of transparency as per Articles 12 to 14 of Regulation (EU) 2016/679 (GDPR), will be published with the CGSD authorisation, is attached to the application. *
Data Holder 1 ✓	
Description of the context of access to and re-use of data ✓	
Description of data categories ✓	

The “Impact Assessment and Information Notice” section of the Application for Re-Use of Data will be shown and must be completed, if you have requested that the data be made available in the SPE in a pseudonymised format. If pseudonymised data is processed in the SPE, you must, in principle, comply with the rules on data protection (see section 3.2.1.3 of the User Guide).

This entails that you must carry out **a DPIA** and draw up **[a data protection notice for the Data Subjects](#)**, both of which must be attached to your Application for Re-Use of Data.

The **DPIA** must be carried out to demonstrate that the risks to the rights and freedoms of the Data Subjects can be considered to be minimal.¹⁹ It must contain at least:

- (a) a systematic description of the envisaged processing activities and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
- (b) an assessment of the necessity and proportionality of the processing activities in relation to the purposes;
- (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and
- (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR. In this regard, make sure that the measures described in the DPIA are aligned with those defined in the [Appropriate Measures Plan](#).

The **data protection notice** should comply with Articles 12 to 14 of the GDPR. Please pay particular attention to the provisions of Article 14 of the GDPR, as the Personal Data will mostly not be collected directly from the Data Subjects.

For more information on the DPIA and the information notice, please see:

- [The EDPS Guidelines on Data Protection Impact Assessment \(DPIA\) and how to determine whether processing is “likely to result in a high risk” for the purposes of Regulation \(EU\) 2016/679 \(WP 248\)](#)
- [The EDPB DPIA Template \(version published for public consultation\)](#)
- [The guidance of the National Commission for Data Protection \(CNPD\)](#)
- [The EDPS Guidelines on transparency within the meaning of Regulation \(EU\) 2016/679 \(WP 260rev.01\)](#)

¹⁹ DGA, recital 15.

5.12 Secure Processing Environment (ETS)

The SPE is a digital environment designed to ensure safe, compliant and efficient use of Target Data. Once your Application for Re-Use of Data has been authorised, the Target Data will be made available in the SPE.

5.12.1 Internal Technological Solutions

Application for re-use of data (Data Factory)

Steps filling	Secure processing environment
Information ✓	The different standard technological solutions available in the secure processing environment can be viewed here. Technological solution Select the technological solution to be requested * Default environment ▾ Type of result envisaged * 0/250
Contact person ✓	
Applicant(s) ✓	
Data Holder 1 ✓	
Description of the context of access to and re-use of data ✓	
Description of data categories ✓	
Lawfulness ✓	
Appropriate Measures ✓	
Data use and retention periods ✓	
Data users ✓	
Rights and freedoms ✓	

The technological solutions proposed under the 'Technological solution' tab currently correspond to standard solutions. You can consult the list of standard Internal Technological Solutions [here](#).

In the 'Type of expected result' field, you should describe the type of expected result (e.g. statistical report, AI model, etc.).

5.12.2 Addition of External Technological Solutions

Secure processing environment

Addition by the Applicant(s) of technological solutions/features in the secure processing environment

☒ We wish to use one or more technological solution(s) not included in the previous list

Name(s) of the technological solution(s) * 0/3500

Description of the envisaged technological solution(s) * 0/3500

If you wish to request the addition of **External Technological Solutions** into the ETS, please tick the box provided for this purpose and describe the External Technological Solution(s) you wish to integrate.

At this stage of the Application for Re-Use of Data, you are not required to provide the CGSD with the External Technological Solution(s) envisaged. However, you may be asked for additional information at a later stage, in particular to carry out an independent audit of the External Technological Solution(s). This audit must be carried out by an external auditor appointed by the CGSD, and all costs relating to this audit shall be at your charge.

If, in the course of the project, you consider that another External Technological Solution is necessary, you may submit a specific request to that effect to the CGSD.

Please note that the addition of External Technological Solutions remains subject to the technical and organisational capabilities of the CGSD (e.g. a script can be validated more easily than a certain software).

For further information on the use of the SPE, please refer to the [dedicated user guide](#) as well as the [general conditions of use of the secure IT environment](#).

5.13 Validation and signatures

Application for re-use of data (Data Factory)

Steps filling

Information	✓
Contact person	✓
Applicant(s)	✓
Data Holder 1	✓
Description of the context of access to and re-use of data	✓
Description of data categories	✓
Lawfulness	✓
Appropriate Measures	✓
Data use and retention periods	✓
Data users	✓
Rights and freedoms	✓
Secure processing environment	✓
Confirm the entry	

Confirmation of input

Your procedure has not yet been submitted.

Please review all of the entered information.

Click 'Continue' to confirm, or 'Back' to edit your input.

Information	▼
Contact person	▼
Applicant(s)	▼
Data Holder 1	▼
Description of the context of access to and re-use of data	▼
Description of data categories	▼
Lawfulness	▼
Appropriate Measures	▼
Data use and retention periods	▼
Data users	▼
Rights and freedoms	▼
Secure processing environment	▼

When you have completed the Application for Re-Use of Data form on MyGuichet and verified the accuracy of the data entered, you can generate a PDF of the completed application.

The PDF must be signed by **all Applicants and Data Holders**, either by hand or electronically.

- Handwritten signature: upload a copy of the duly signed form and send the original by post to the CGSD (Government Commission for data sovereignty, Luxembourg Data Authority, 5, rue Plaetis, L-2338 Luxembourg).
- Electronic signature: the application form must be signed by means of a qualified electronic signature and uploaded with the qualified certificate, where applicable.

By signing the Application for Re-Use of Data, you confirm that:

- you have read the data protection notice concerning the processing of your Personal Data by the CGSD,
- you have read and accept the general terms and conditions of the secure IT environment (SIE),
- all the information provided in the Application for Re-Use of Data, including in the attachments, is accurate and up-to-date,
- you have not amended or replaced any documents attached to the Application for Re-Use of Data following signature by the Data Holder(s).

Providing inaccurate information may entail the rejection of the Application for Re-Use of Data.

The person(s) acting in the name and on behalf of the Data Holder(s) must also confirm having signing authority for the Data Holder in question and having read all the supporting documents attached to the Application for Re-Use of Data.

5.14 Attachments

Home > My procedures > Application for re-use of data (Data Factory)

Application for re-use of data (Data Factory)

Step 3/4

In preparation

Show the steps



LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de la Digitalisation
Commissariat du gouvernement
à la souveraineté des données

Contact

Commissariat du Gouvernement à la souveraineté des données

Show the contact details

Overview

File

Message

History of the procedure

Find out more about this procedure

Your opinion matters to us

Please give us your feedback on this procedure.
You can give us suggestions on how we can improve.

I would like to leave a comment

File

TOTAL: 1 form, 0 annex, 7 attached documents

Mandatory*

Form

Application for re-use of data (Data Factory)

Ready

Edit

Attached documents

DPiA

Data protection impact assessment (DPiA)

Attached

Replace

Notice

Information notice for data subjects

Attached

Replace

Analysis of legitimate interests

Analysis of legitimate interests

Attached

Replace

Appropriate Measures Plan

Appropriate Measures Plan

Attached

Replace

Data description

Data description

Attached

Replace

Signed application form

Signed application form

Attached

Replace

User List

User list

Attached

Replace

Add an attachment

or drag and drop your documents.

Message

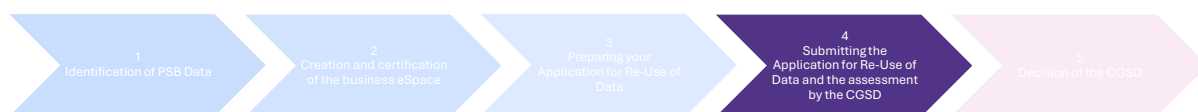
Send

Before sending the Application for Re-Use of Data to the CGSD, check that all the supporting documents have been uploaded:

Copy of the Application for Re-Use of Data signed by all Applicants and Data Holders in accordance with section 5.13	Mandatory
Appropriate Measures Plan	Mandatory
Data Description	Mandatory
User List	Mandatory
Agreement between the joint controllers	Mandatory in case of multiple Applicants who request access to data in pseudonymised format. To add this item, click on the 'Add attachment' tab.
Analysis of legitimate interests	Mandatory where the Data is requested in pseudonymised format and the processing is based on Article 6.1(f) of the GDPR
Information Notice for Data Subjects	Mandatory when data is requested in pseudonymised format
Data protection impact assessment	Mandatory when data is requested in pseudonymised format

When analysing your Application for Re-Use of Data, the CGSD may request additional information.

6 Submitting the Application for Re-Use of Data and the assessment by the CGSD



6.1 Submitting the Application for Re-Use of Data

When all necessary supporting documents have been uploaded, you can send the Application for Re-Use of Data to the CGSD.

After submission, you will receive a proof transmission, as shown in the example below:

6.2 Assessment by the CGSD

Upon receipt, the CGSD reviews your Application for Re-Use of Data to assess its admissibility, verify that it is complete and ensure compliance with the applicable requirements.

Next, the CGSD assesses the merits of the Application for Re-Use of Data by verifying whether the conditions applicable to re-use, as set out in the DGA and the Law, are met. Where appropriate, the CGSD may delegate the following assessments to processors:

- a theoretical analysis of the proposed Appropriate Measures, and/or
- a theoretical analysis of the External Technological Solutions requested.

6.3 Duration of assessment of the Application for Re-Use of Data

The two-month assessment period for the Application for Re-Use of Data begins only after the CGSD has received all the information necessary for its assessment.

In the event of an exceptionally extensive and complex Application for Re-Use of Data, this period may be extended by a maximum of thirty days. You would then be informed of the extension and the reasons for it.

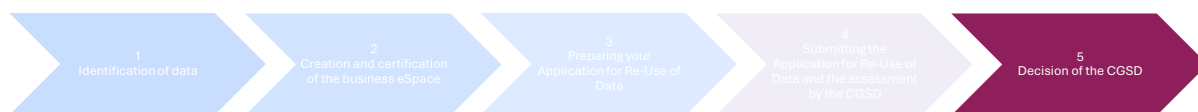
6.4 Request for additional information

To process your Application for Re-Use of Data, the CGSD may need additional documents or information (e.g. information about an External Technology Solution you wish to use in the SPE, etc.).

Any request for additional information will be sent to you via MyGuichet, and your response should also be submitted through this channel.

Please note that the CGSD will not be able to process your Application for Re-Use of Data if no response is received.

7 Decision of the CGSD



7.1 Adoption and notification of the decision

When the CGSD has concluded its assessment of the Application for Re-Use of Data, a decision authorising or refusing the access to and re-use of data is issued.

The CGSD notifies its decision to the Applicant, who submitted the Application for Re-Use of Data, via the MyGuichet.lu certified business eSpace.

This decision may be appealed, as provided for by the Luxembourg administrative law in force.

7.2 Publication of the decision

In parallel with the notification of the decision, the CGSD publishes, on the [website LetzData.lu](https://www.letzdata.lu):

- the authorisation or refusal decision;
- a copy of the Re-User(s)'s data protection notice for the Data Subjects, in line with Articles 12 to 14 of the GDPR;
- a copy of the CGSD data protection notice.