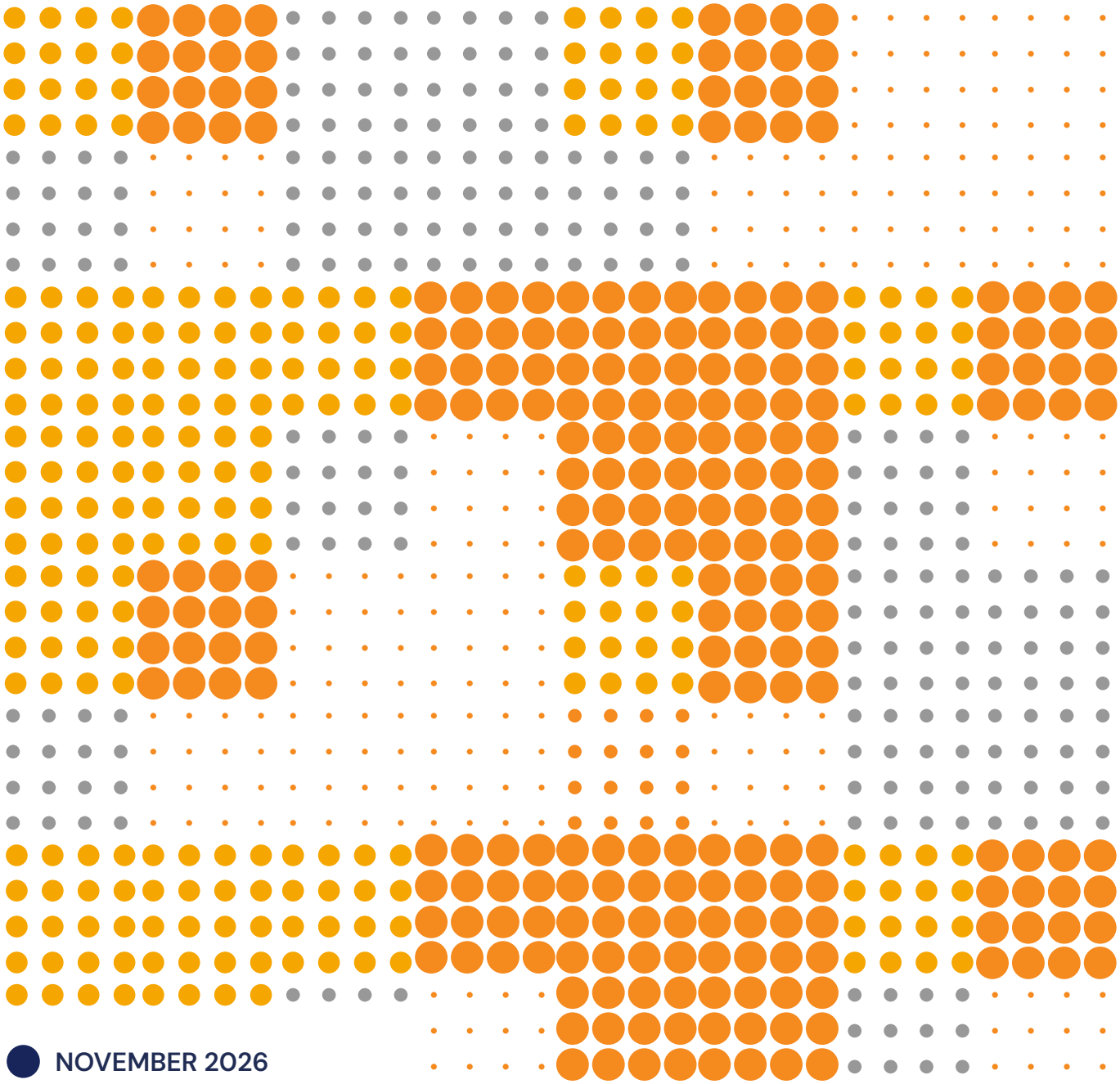
agencia española protección datos

HELLENIC DATA PROTECTION AUTHORITY

SECURE PROCESSING ENVIRONMENTS FROM THE DATA PROTECTION PERSPECTIVE



NOVEMBER 2026

This document has been collaboratively prepared by the data protection authorities of Spain and Greece.

Main authors:

- On behalf of the Spanish Data Protection Authority (AEPD): the Technological Innovation Division, represented by Luis de Salvador Carrasco and Teresa Martínez Sánchez.
- On behalf of the Hellenic Data Protection Authority (HDPA): the Research and Studies Dept., represented by Konstantinos Limniotis and Eleni Maragou.

Reviewers:

The document has benefited from the valuable contributions of the following experts during its review:

- Fabio Ricciato (Eurostat, European Commission).
- Giuseppe D'Acquisto (Italian Data Protection Authority "*Garante per la protezione dei dati personali*", Italy).
- Carlos Alonso Peña and Guillermo Pérez de Arenaza Pozo (General Directorate for Data, Ministry for Digital Transformation and the Civil Service, "*Dirección General del Dato, Ministerio para la Transformación Digital y de la Función Pública*", Spain).
- Paul Comerford (Information Commissioner's Office, United Kingdom).

TABLE OF CONTENTS

LIST OF ACRONYMS 5

EXECUTIVE SUMMARY 6

I. INTRODUCTION 7

II. WHAT IS SECURE PROCESSING ENVIRONMENT 8

A. DEFINITION AND LEGAL REFERENCE 8

1. DGA 8

2. EHDS 11

3. OTHER REGULATIONS 12

B. SPES AND DATA PROTECTION COMPLIANCE 12

1. ROLE DEFINITION IN SPES 13

2. CONTRACTUAL TERMS AND ALLOCATION OF RESPONSIBILITIES 13

3. THIRD PARTIES AND THE SPE IMPLEMENTATION 14

4. INTERNATIONAL TRANSFERS 17

5. FACILITATING THE EXERCISE OF DATA SUBJECTS' RIGHTS 17

6. PRIVACY BY DESIGN AND BY DEFAULT 18

7. DATA PROTECTION RISKS MANAGEMENT 21

III. IMPLEMENTATION CONSIDERATIONS AND MEASURES 25

A. MEASURES THAT SHALL BE IMPLEMENTED 25

1. GOVERNANCE AND ACCOUNTABILITY 25

2. DATA MANAGEMENT 26

3. IDENTITY MANAGEMENT AND ACCESS CONTROL 27

4. PHYSICAL SECURITY 27

5. NETWORK AND COMMUNICATIONS SECURITY 27

6. SYSTEM AND APPLICATIONS SECURITY 28

7. AUDIT, LOGGING, MONITORING 28

8. INCIDENT RESPONSE, RECOVERY AND RESILIENCE 29

9. MANAGEMENT OF THIRD PARTIES 29

10. ORGANISATIONAL CULTURE AND TRAINING 29

B. DATA PROTECTION ENGINEERING TO IMPLEMENT A SPE 30

1. SPES VS TEES 30

2. HOMOMORPHIC ENCRYPTION 30

3. SECURE MULTY-PARTY COMPUTATION 31

4. POLYMORPHIC ENCRYPTION AND PSEUDONYMISATION 32

5. OBLIVIOUS PSEUDONYMISATION 33

6. DIFFERENTIAL PRIVACY 33

7. FEDERATED LEARNING 34

C. MAPPING THREATS AND MEASURES 34

IV. A USE-CASE SCENARIO 35

A. DESCRIPTION OF THE SCENARIO 35

B. DATA PROTECTION RISKS ANALYSIS (RELATED TO LINKING) 36

C. DATA PROTECTION ENGINEERING APPROACH 37

D. THE DATA PROTECTION ENGINEERING TECHNIQUE IN DETAIL 37

1. STEP 1: AGREEMENT AND SETUP 37

2. STEP 2: CRYPTOGRAPHIC KEYS MANAGEMENT 37

3. STEP 3: SENDING ENCRYPTING DATA TO THE HDAB 38

4. STEP 4: SECURE COMPUTATION VIA HDAB 38

5. STEP 5: SHARING RESULTS 38

6. STEP 6: ANALYSIS AND REPORTING 38

V. FINAL REFLECTIONS 40

VI. REFERENCES 42

LIST OF ACRONYMS

AI	Artificial Intelligence
DA	Data Act
DGA	Digital Governance Act
DLP	Data Loss Prevention
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EDPB	European Data Protection Board
EHDS	European Health Data Space
ENISA	European Union Agency for Cybersecurity
FAIR	Findability, Accessibility, Interoperability, and Reusability
FL	Federated Learning
GDPR	General Data Protection Regulation
HDAB	Health Data Access Body
HE	Homomorphic Encryption
MFA	Multi-factor Authentication
NIST	National Institute of Standards and Technology
PoLP	Principle of least privilege
SPE	Secure Processing Environment
TEE	Trusted Execution Environment
VDI	Virtual Desktop Infrastructure

EXECUTIVE SUMMARY

Secure Processing Environments (SPEs) enable controlled access to data under conditions designed to safeguard the rights and freedoms of individuals and protect the legitimate interests of data holders, without relying exclusively on the legal, organisational or technical safeguards implemented by data users. Such enhanced guarantee is essential to fostering trust in the data-driven economy and strengthening confidence among individuals and undertakings in the secure and responsible use of data. In particular, SPEs support a shift from traditional data sharing towards controlled data access, allowing authorised processing without necessarily transferring the underlying data to data users. The Data Governance Act (DGA) and the European Health Data Space Regulation (EHDS) establish a framework with the aim to facilitate access to protected or sensitive data while safeguarding fundamental rights and other legitimate interests.

This report examines SPEs from a data protection perspective, focusing on their legal, organisational and technical dimensions. Its objective is to provide high-level guidance on the considerations and safeguards relevant to their design, implementation and operation, particularly within the frameworks of the DGA and the EHDS.

To this end, the report stresses that the design and implementation of SPEs require a comprehensive approach that combines legal, organisational and technical safeguards, extending beyond conventional cybersecurity measures. Its implementation must ensure compliance with the General Data Protection Regulation (GDPR), including data protection by design and by default, accountability, data minimisation and the effective exercise of data subjects' rights. Particular emphasis is placed on the need for the entity responsible for the SPE to retain genuine and effective control over processing operations, including when infrastructure or services are provided by third parties. Contractual assurances alone may be insufficient unless supported by appropriate technical measures, effective oversight and audit capabilities.

The report also emphasises the importance of a comprehensive and integrated risk management approach that extends beyond conventional cybersecurity and personal data protection risks. SPEs must address, in a context specific approach, a broad range of interconnected risks, including those relating to other fundamental rights, third-party dependencies and digital sovereignty. Moreover, evolving technological, geopolitical and legal developments may introduce additional threats that need to be considered. Since risks arising in one area may also affect personal data protection, their assessment should not be conducted in isolation, but within a unified risk management framework. In this context, Data Protection Impact Assessments (DPIAs) play a central role in identifying and addressing risks to individuals' rights and freedoms, while contributing to the selection of appropriate safeguards.

Beyond conventional security measures, the report explores how advanced data protection engineering techniques, including homomorphic encryption, secure multi-party computation, oblivious pseudonymisation and federated learning, can strengthen privacy safeguards. These techniques may enable authorised computations while limiting access to underlying personal data, although their suitability and limitations must be assessed in each specific context. An illustrative health research use case demonstrates how homomorphic encryption can support statistical analysis across multiple data sources without requiring the disclosure of original data to the SPE provider or the researchers.

This report provides initial guidance for entities acting as controllers in the context of data access and processing through SPEs, as well as for Data Protection Officers (DPOs), data protection advisors, and stakeholders involved in the design, deployment and operation of such environments. Its purpose is to facilitate the effective implementation of SPEs, guided by data protection principles and appropriately embedded in their design. This approach is complemented by a comprehensive strategy to identify and manage the wide range of risks associated with their design, deployment and operation.

I. INTRODUCTION

The Data Governance Act[1] (hereinafter DGA) and the European Health Data Space Regulation[2] (hereinafter EHDS) aim to establish a common European vision for the development of an open, federated, and trustworthy data ecosystem. This vision is based on the principle of data sovereignty, ensuring that data holders[3] and data subjects[4] retain effective control over how data are accessed and used[5]. To achieve this objective, both regulations promote the creation of interoperable infrastructures supported by governance policies, rules, and standards that collectively define a trusted framework for all stakeholders. This framework is implemented through a combination of organisational, legal, and technical measures designed to enable data reuse while safeguarding fundamental rights, economic interests, and public policy objectives and, specifically and explicitly, the rights and freedoms of the data subjects regarding the processing of their personal data.

In addition to concerns regarding personal data protection, data reuse entails a wide range of risks that should also be taken into consideration. These risks may affect trade and statistical secrets, intellectual and industrial property rights, national security interests, public policies, and the confidentiality obligations of data holders.

Both the DGA and the EHDS identify situations in which the organizational, legal, or technical safeguards that data users[6] may provide are insufficient to ensure the protection of data holders' interests, and to achieve the objectives pursued by these regulations when granting access to data, inter alia, trust to all the stakeholders. Regardless of the nature of the data user (whether a private entity, a public body, or an individual researcher), certain circumstances require the implementation of stronger safeguards to govern data access and reuse. Such enhanced guarantees are essential to fostering trust in the data-driven economy and strengthening confidence among individuals and undertakings in the secure and responsible use of data. Drawing on the practical experience acquired through several European initiatives in both statistical and health domains, providing indicative examples in practice, Secure Processing Environment infrastructure (hereinafter, "SPE") emerges as a solution[7].

The goal of the SPE is to ensure legal compliance and digital sovereignty for the entity that provides it without the need of relying on the guarantees offered by the data user. A SPE is not a single technological solution or product, but rather a comprehensive set of organisational, legal, and technical measures that together create a controlled environment for data processing while enabling the analysis and reuse of data (particularly sensitive or specifically protected data). SPE is one of the ways to implement the access-based model, the concept of "data access" as is laid

[1] Regulation (EU) 2022/868 of the European Parliament and of the Council, of 30 May 2022, on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R0868)

[2] Regulation (EU) 2025/327 of the European Parliament and of the Council, of 11 February 2025, on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202500327)

[3] Article 2(8) of DGA: "'data holder' means a legal person, including public sector bodies and international organisations, or a natural person who is not a data subject with respect to the specific data in question, which, in accordance with applicable Union or national law, has the right to grant access to or to share certain personal data or non-personal data;"

[4] Article 4(1) of GDPR: "(...) identified or identifiable natural person ('data subject');"

[5] This vision was first set out in "A European strategy for data" [Feb 2020] (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0066) and is being continued in the "Data Union Strategy. Unlocking Data for AI" [Nov 2025] (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52025DC0835).

[6] Article 2(9) of DGA: "'data user' means a natural or legal person who has lawful access to certain personal or non-personal data and has the right, including under Regulation (EU) 2016/679 in the case of personal data, to use that data for commercial or non- commercial purposes;"

[7] Notable examples include Eurostat's "KIOSK" (European Statistical System Trusted Research Environment), Spain's INE Secure Data Centers, France's CASD (Centre d'Accès Sécurisé aux Données), French Health Data Hub (HDH), Spain's BELab, Portugal's BPLIM, Finland's Findata, and the UK's NHS Trusted Research Environments.

down in the DGA, where the data remain under the control of the data holder, and the data user is granted the ability to perform authorised processing operations within predefined boundaries.

DGA states that, in certain cases, data can be used and re-used only in a SPE that is provided or controlled by the public sector body[8]. But it is in the context of the EHDS where SPEs acquire particular significance. The aim of EHDS is to improve natural persons' access to and control over their personal electronic health data in the context of healthcare (primary uses), as well as to better achieve other purposes involving the use of electronic health data in other sectors that would benefit society (secondary uses). The EHDS establishes that access to electronic health data for secondary purposes must be carried out through SPEs[9] as "*an essential safeguard to preserve the rights and freedoms of natural persons in relation to the processing of their electronic health data for secondary use*". This reflects the high sensitivity of health data, the subsequent requirement for enhanced level of protection and the corresponding need for robust technical and organisational safeguards that go beyond traditional access control mechanisms.

The EHDS further clarifies the relationship between SPEs and the General Data Protection Regulation[10] (hereinafter GDPR). Recital (77) specifies that the processing of personal data within a SPE must comply fully with GDPR. As such, SPEs are not an alternative to GDPR compliance, but rather a means of operationalising data protection principles in complex, large-scale data processing scenarios. Importantly, SPEs are not mutually exclusive with other privacy-enhancing or security-preserving techniques. On the contrary, they can be used in combination with complementary measures such as anonymisation, pseudonymisation, differential privacy, federated processing, secure multi-party computation, homomorphic encryption, and other advanced technologies, depending on the risk profile and intended use of the data.

The scope of this guide is to provide a high-level analysis of the organisational, legal, and technical requirements that secure processing environments should fulfil in order to manage risks to personal data protection effectively. It does not assess specific implementations or prescribe detailed technical or organisational approaches for the design and deployment of such environments. As an initial guiding document, it is intended simply to support understanding of the concept and should not therefore be interpreted as an exhaustive statement of requirements. Although a SPE is a type of infrastructure that can be implemented in different contexts, this text focuses on SPEs in processing activities within the scope of the DGA and the EHDS.

II. WHAT IS SECURE PROCESSING ENVIRONMENT

This section examines the scope of the definition of SPEs across various European legal frameworks, and analyses a series of relevant data protection considerations within these environments.

A. Definition and legal reference

1. DGA

The DGA provides the formal EU-level definition of a Secure Processing Environment (SPE). Article 2(20) describes a SPE as a "*physical or virtual environment and organisational means to ensure*

[8] Article.5(3)(b) and Recital (7) of DGA.

[9] Article 73 and Recital (77) of EHDS.

[10] 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) (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679)

compliance with Union law, such as Regulation (EU) 2016/679, in particular with regard to data subjects' rights, intellectual property rights, and commercial and statistical confidentiality, integrity and accessibility, as well as with applicable national law, and to allow the entity providing the secure processing environment to determine and supervise all data processing actions, including the display, storage, download and export of data and the calculation of derivative data through computational algorithms".

As defined by DGA, SPE in an infrastructure that ensures legal compliance for the entity that provides it **without the need of relying on the guarantees offered by the data users** whether the data user is a private entity, a public body, or an individual researcher. By enabling such control and supervision over data processing operations, the SPE may also be understood as supporting digital sovereignty for the entity providing it. In practical terms, a SPE is more than a way to implement the "FAIR data principles"[11] and cybersecurity but a controlled infrastructure, whether a secure physical facility or a virtual platform, designed to ensure that sensitive data is processed under strict technical and organizational safeguards[12]. A key element of the definition is the SPE provider's ability to maintain effective oversight of every operation performed within the environment, from data access and visualization to transformation and output generation. SPEs thus function not only as secure IT systems but as comprehensive compliance frameworks.

SPEs allow the implementation of the data access model rather than a traditional data sharing model, reflecting a key conceptual distinction underpinning the DGA and the EHDS. According to Article 2(10) of the DGA, "data sharing" refers to the provision of data by a data subject or data holder to a data user for joint or individual use, based on voluntary agreements or legal obligations, and may involve the transmission of data directly or through an intermediary. Traditional data sharing inherently implies that copies of the data are transferred or made available to the data user, who may then process them within their own systems, subject to contractual or legal constraints. By contrast, Article 2(13) of the DGA defines "access" as the use of data in accordance with specific technical, legal, or organisational requirements, without necessarily implying the transmission or downloading of the data. In an access-based model, the data remain under the control of the data holder, and the data user is granted the ability to perform authorised processing operations within predefined boundaries.

SPEs play a pivotal role in enabling access, rather than traditional data sharing, particularly for protected or sensitive datasets. Historically, once data are transferred outside the systems of the original holder, supervising or limiting their subsequent use became difficult. SPEs aim to fundamentally alter this paradigm by shifting from "moving the data" to "bringing the user to the data". All processing takes place within a tightly controlled environment where access is restricted, user actions are logged and monitored, and unauthorised outputs are technically prevented.

As laid down in recital (7) of the DGA "*in many cases the application of such techniques [anonymisation, differential privacy, generalisation, suppression and randomisation, the use of synthetic data or similar methods and other state-of-the-art privacy-preserving methods that could contribute to a more privacy-friendly processing of data], impact assessments and other*

[11] To make data Findable, Accessible, Interoperable and Reusable. https://force11.org/info/the-fair-data-principles/

[12] The proper implementation of SPEs is essential in order to meet the requirements set out to achieve the technical sovereignty objectives outlined in the "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on European Tech Sovereignty, accompanied by an EU Open Source Strategy" (COM(2026) 503 final) (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52026DC0503), and in particular the following:
"II) securing the supply of digital technologies underpinning Europe's competitiveness including by diversifying supply chains and reducing dependencies particularly on a single or a limited number of non-EU suppliers, including via trusted trade and investment partnerships;
III) gain and maintain control over data infrastructures and critical data, while developing the capacity to effectively leverage them;"

safeguards implies that data can be used and re-used only in a secure processing environment that is provided or controlled by the public sector body" therefore the DGA positions SPEs as the principal mechanism for enabling the re-use of protected public-sector data, including personal data, trade secrets and confidential statistics[13], and certain types of non-personal data that may be identified as highly sensitive (for example in the health domain, transport, energy, environment and finance)[14].

Under Article 5(3) of the DGA, public sector bodies are required to preserve the protected nature of data during re-use, providing for three distinct approaches. The first involves pre-processing data (e.g. anonymizing personal data or applying disclosure control methods like aggregation or modification). However, when these measures prove insufficient or impractical, the DGA emphasizes SPE-based solutions for the remaining two approaches. More precisely, Article 5(3) states that public sector bodies may provide for the following requirements: *(a) (…), (b) to access and re-use the data remotely within a secure processing environment that is provided or controlled by the public sector body; (c) to access and re-use the data within the physical premises in which the secure processing environment is located in accordance with high security standards, provided that remote access cannot be allowed without jeopardising the rights and interests of third parties*". Therefore, in both SPE-based scenarios, the environment serves as a technical and organizational safeguard, ensuring that sensitive data (whether personal, commercial, or statistical) can be processed and re-used without ever leaving a supervised and controlled space.

Access to such data may be granted solely within a SPE controlled by the public-sector body[15], ensuring that information always remains in a monitored and safeguarded space. In essence, the DGA frames SPEs as a set of legal, organizational and technical instruments that implement data sovereignty and reconcile data access with robust protections for trade secrets, intellectual property and *commercial and statistical confidentiality*, while safeguarding legitimate Union public policy objectives identified, such as the protection of public health, safety, the environment, public morality, consumer protection, privacy and personal data protection (AEPD, Data Spaces, sovereignty and privacy by design, 2023).

Recital (7) of DGA states that "*In many cases the application of such techniques, impact assessments and other safeguards implies that data can be used and re-used only in a secure processing environment that is provided* ***or controlled*** *by the public sector body.*" and, therefore, open the chance that a SPEs is implemented by a third party under the control of the public sector body. However, the involvement of such a third party does not, by itself, determine its role under the GDPR, nor would it necessarily mean that this third party could have the role of processor. In such cases, the guarantees, safeguards and control over the processing operations by the third party required by the entity in charge of the SPE should be more robust and extensive that the ones required to a data user.

More precisely, the notion of "control" should not be understood solely in legal terms (*de iure* control), i.e., as the legal authority to determine how the SPE and the data made available within it may be used. Such authority should be accompanied by effective control in practice (*de facto* control), supported by appropriate technical and organisational measures that enable the entity in charge of the SPE to determine, restrict, supervise and, where necessary, prevent processing operations. Therefore, particular attention should be paid where a third-party provider has the technical capability to access or process data independently of the entity in charge of the SPE, especially where it is subject to the laws of a non-EEA country.

[13] Recital (7) of DGA.

[14] Recital (24) of DGA.

[15] Recital (15) of DGA.

This approach aims to strengthen trust between data holders[16] and data users[17], while simultaneously ensuring the protection of the rights of data subjects[18]. In other words, legal requirements should be supported and effectively enforced through appropriate technical measures: what is legally prohibited should, to the extent possible, also be technically prevented. Technical controls should therefore complement and give effect to legal controls. Public authorities, healthcare institutions and private companies can be confident that data is used only for the authorized purpose, while researchers gain access to datasets that would otherwise remain unavailable.

2. EHDS

Likewise, the EHDS Regulation builds directly on the DGA's concept of SPEs. The EHDS further develops and specifies certain aspects of the DGA for the particular context of health data and their secondary use.

Secondary use of health data is laid down in Chapter IV of EHDS and explained in recital 61 "*The secondary use of health data under the EHDS should enable public, private and not-for-profit entities, as well as individual researchers, to have access to health data for research, innovation, policymaking, educational activities, patient safety, regulatory activities or personalised medicine, in line with the purposes as set out in this Regulation. Access to data for secondary use should contribute to the general interest of society.*" Given the heightened sensitivity of electronic health data, the EHDS introduces more detailed governance rules and safeguards, in which SPEs play a central role as a key mechanism to enable controlled access while ensuring a high level of protection.

As laid down in Article 73, all secondary use of electronic health data must occur exclusively within a SPE governed by a Health Data Access Body[19] (hereinafter HDAB). This means researchers and research entities get access to the datasets but, as laid down in Article 73(2), without chance to download personal data[20]. As detailed in paragraph 1 of Article 73, the EHDS requires strict safeguards for SPEs, including: access limited to authorized individuals listed in the data permit, state-of-the-art protection against unauthorized reading, copying, or removal, and a minimal number of authorised identifiable individuals allowed to input, inspect, delete or modify data. SPEs must maintain comprehensive, auditable logs retained for at least one year, restrict users to only the data necessary for their approved purpose, and prevent any export of personal data (only anonymized, checked outputs may leave the environment)[21].

Article 51(1) of EHDS outlines the minimum categories of electronic health data for secondary use, which, in addition to those related to electronic health records, also include other categories such as personal electronic health data automatically generated through wellness applications or registries for medicinal products; nonetheless, it is important to take into account that Article 51(4)

[16] Article 2(8) of DGA for data holder definition.

[17] Article 2(9) of DGA for data user definition.

[18] Recital (5) of DGA stablishes that "A Union-wide governance framework should have the objective of building trust among individuals and undertakings in relation to data access, control, sharing, use and re-use, in particular by establishing appropriate mechanisms for data subjects to know and meaningfully exercise their rights, as well as with regard to the re-use of certain types of data held by the public sector bodies, the provision of services by data intermediation services providers to data subjects, data holders and data users, as well as the collection and processing of data made available for altruistic purposes by natural and legal persons"

[19] See Chapter IV "Secondary Use", Section 2 "Governance and mechanisms for secondary use" of EHDS for detailed description of the Health Data Access Body.

[20] *"Health data access bodies shall review the electronic health data included in a download request to ensure that health data users are only able to download non-personal electronic health data"*

[21] https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space-regulation-ehds_en#:~:text=Data%20processing%20can%20only%20take,these%20stringent%20measures%20are%20essential

lays down that "*Member States may introduce stricter measures and additional safeguards at national level aimed at safeguarding the sensitivity and value of the data that fall under paragraph 1, points (f) [human genetic, epigenomic and genomic data], (g) [other human molecular data such as proteomic, transcriptomic, metabolomic, lipidomic and other omic data], (i) [data from wellness applications] and (q) [health data from biobanks and associated databases]*". This is an additional criterion to assess when data sets (total or partially) should be considered under special protection.

3. Other regulations

Another relevant legal instrument is the Data Act[22] which governs access to data from connected devices and other business-to-business data sharing. The Data Act reinforces the role of SPE-like safeguards in industrial and IoT data sharing. Although it does not define SPEs nor explicitly mention it, article 4(6) requires parties sharing data containing trade secrets to agree on proportionate confidentiality measures, thus stating the use of technical and organisational measures, a provision which alludes to a secure processing environment solution. In practice, this allows data holders to require that sensitive business data be analyzed only within a controlled, access-restricted environment and to suspend sharing if safeguards are breached. The Data Act therefore implicitly endorses SPEs as mechanisms to facilitate data portability while protecting intellectual property and confidential know-how.

Sector-specific legislation may also considered to reflect in some rudimentary form the principles of the SPE model. For instance, under the European Statistics framework[23] researchers may access confidential microdata only under strict conditions, often via secure on-site centers or remote-controlled facilities structures; one could say that this prefigures the SPE concept later formalized in the DGA.

B. SPEs and Data Protection Compliance

A SPE is an **infrastructure that enables access to and the processing of sensitive data.** In addition, the **management and operation of the SPE will involve the processing of personal data to ensure the proper operation** of the SPE and, among other objectives, to support accountability, privacy and security[24].

As laid down in Article 1 of the DGA and Article 2(1)a) and (3) of the EHDS, the processing of personal data within a SPE must fully comply with GDPR. This clarification confirms that the use of SPE does not alter the allocation of roles and responsibilities under the GDPR, nor does it exempt controllers or processors from their legal obligations. Consequently, all GDPR principles applicable

[22] 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) (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202302854)

[23] See:
- Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No 322/97 on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32009R0223)
- Commission Regulation (EU) No 557/2013, of 17 June 2013, implementing Regulation (EC) No 223/2009 of the European Parliament and of the Council on European Statistics as regards access to confidential data for scientific purposes and repealing Commission Regulation (EC) No 831/2002 (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32013R0557)

[24] For example, in the case of IT infrastructures supporting the healthcare sector for processing involving electronic health records, electronic prescriptions, etc., it is also necessary to manage the data of the users of that infrastructure, ranging from the data of IT staff responsible for the development and maintenance of the infrastructure, to the data of healthcare system personnel and beneficiaries of the healthcare system, etc.

to the controller must be effectively implemented, including lawfulness, fairness and transparency, purpose limitation, data minimisation, integrity and confidentiality, and, in particular, the principle of accountability enshrined in Article 5(2) of GDPR (AEPD, 2023). Controllers must be able to demonstrate compliance with these principles through appropriate technical and organisational measures.

Appropriate governance of a SPE entails establishing controlled mechanisms for data access that ensure legal compliance and digital sovereignty. SPEs face significant organizational challenges, particularly in relation to governance structures and the management of processors and intermediaries. Effective governance is essential to ensure compliance with data protection legal requirements.

Specifically for GDPR compliance, comprehensive governance frameworks should be established to implement the accountability principle, including clearly defined roles, responsibilities, and mechanisms for overseeing secure data processing operations.

1. Role definition in SPEs

EHDS, in Article 74 and Recital (79), clearly defines the GDPR's roles by processing activities regarding with SPE in the following way:

- The HDAB is the controller of the personal data processed in the SPE with the purposes to fulfill its tasks pursuant to the EHDS regulation.
- The HDAB acts as processor on behalf of the health data user acting as a controller for the processing of the personal electronic health data pursuant to a data permit issued under Article 68 of EHDS.
- In the last case, health data user acts as controller of such processing activities.
- The trusted health data holder shall be deemed to act as a processor on behalf of the health data user when providing data through a SPE.

Such roles are not defined in the more general case of the SPEs in the framework of DGA, and cannot be assumed to be uniform, as each case requires an individual, contextual and detailed assessment that takes into account the specific characteristics of the infrastructure defined for each data space; although the role assignments set out by EHDS could be used as guidance. Anyway, the role of the data controller, including possible situations of joint controllership, should be clearly defined and appropriately documented. This includes explicit clarification of responsibility for tasks such as handling data breaches, responding to data access requests, enabling data subjects to exercise their rights, and providing transparent information to individuals.

2. Contractual terms and allocation of responsibilities

The precise identification of the roles of controller, joint-controllers and processor, together with the corresponding specific clauses, must be explicitly reflected in the contractual arrangements between all parties participating in the SPE, or in any national laws developed in this regard. Contracts should define permissible processing operations, prohibit unauthorised reuse of data[25] and ensure that the SPE provider acts solely on documented instructions, as well as particular clauses regarding the identified risks[26].

[25] In case of using data intermediation services (definition included in Article 2(11) of DGA), the Article 12(a) of DGA lays down that "the data intermediation services provider shall not use the data for which it provides data intermediation services for purposes other than to put them at the disposal of data users and shall provide data intermediation services through a separate legal person"

[26] An initial overview can be found in section III.A of the AEPD's document: "Report of conclusions of AEPD-ENISA's event on data spaces" [Apr 2024] (https://www.aepd.es/documento/report-conclusions-aepd-enisa.pdf)

In Recital (60) and Article 52(4) of the EHDS is laid down that "*Legal, organisational and technical measures to protect intellectual property rights or trade secrets could include common electronic health data access contractual arrangements, specific obligations within the data permit in relation to such rights, pre-processing the data to generate derived data that protect a trade secret but nonetheless have a utility for the health data user or configuration of the secure processing environment so that such data are not accessible to the health data user*".

Contractual governance constitutes a cornerstone of SPE governance implementation. The drafting of contractual terms and conditions raises important legal considerations including in relation to the allocation of responsibilities, liability, audit rights, subcontracting, incident management and termination. These contracts should be customized for each particular case.

At this point, it is important to highlight that the access to health data for secondary purposes is not limited to the framework of the EHDS neither the use of SPE. As is explained in Recital (52) of the EHDS, this regulation regarding use of secondary data is "*Without hindering or replacing contractual arrangements or other mechanisms in place*".

3. Third parties and the SPE implementation

As stated in the DGA, the purpose of a SPE is to enable the entity providing it to ensure legal compliance and maintain digital sovereignty without having to rely on the guarantees provided by data users. Accordingly, where the entity responsible for providing the SPE (in the context of the EHDS, the HDAB) relies on third parties for the implementation or operation of the SPE[27], such arrangements should be structured in a manner that enables the entity to ensure legal compliance[28] and preserve digital sovereignty independently of any guarantees provided by those third parties. It is important to note that a third party does not necessarily assume the role of a processor.

In fact, if we refer back to the definition of SPE set out in Article 2(20) of the DGA, it identifies the need for "*allow[ing] the entity providing the secure processing environment to determine and supervise all data processing actions, including the display, storage, download and export of data and the calculation of derivative data through computational algorithms*" in order, amongst other things, to ensure effective compliance with EU law, and in particular the GDPR. This circumstance requires that the entity providing the SPE (the HDAB in the case of the EHDS) has genuine and effective control over the SPE. Otherwise, the purpose of the SPE would be undermined, as the responsibilities of the entity providing the SPE would effectively be shifted to the third party.

Where the SPE is implemented by a third party, compliance with the requirements applicable to processors under Article 28 GDPR and, where relevant, the provisions on international data transfers set out in Chapter V of the Regulation.

Accordingly, the responsibilities that this entity has under the GDPR (in particular the HDAB in the case of health data) cannot be transferred to the third party solely through contractual safeguards such as those a data user itself might provide, since, under the terms in which the requirements of the EHDS and the DGA itself are set out, these are not sufficient.

The involvement of third-party intermediaries as processors introduces additional organisational governance considerations, as the selection of a processor cannot relax the stringent control requirements that the SPE imposes on data users. A processor may be employed to carry out the data user's management activities without accessing sensitive data, such as health data or others,

[27] As described in Recital (77) of EHDS, SPEs might be managed by third-party entities specifically contracted to provide the technical, organizational and infrastructural tools necessary to perform the required processing operations.

[28] As stated in Recital (7) of DGA "provided or controlled".

including intellectual property. When these entities, which may include external cloud or service providers, are entrusted with processing sensitive data, they should therefore be subject to a rigorous and total control by the HDAB. Maintaining full transparency and control in relation to these entities remains an ongoing challenge, as the principle of accountability continues to apply to the data controller even when some processing activities are outsourced. Consequently, controllers should implement effective monitoring, audit mechanisms[29], and oversight capabilities to verify on a continuous basisthat processors comply with applicable regulatory requirements.

Under the terms set out for SPEs, third-party security certification alone is insufficient, as it does not meet the specific requirements set out in the applicable regulations (specifically, the DGA and the EHDS for health data). The EHDS emphasises the need for effective audit capabilities and full control; as stated in Section II.A.1 this notion should be interpreted as requiring effective, rather than merely nominal, control by the HDAB. Accordingly, contractual provisions defining the HDAB's authority over the SPE should be complemented by appropriate technical measures that enable such authority to be effectively exercised in practice.

In this regard, two distinct considerations should be taken into account. First, reliance on a single vendor should be avoided, where possible, by ensuring that SPE components can be supported by alternative providers, thereby reducing vendor lock-in (ACM, AFM, AP, DNB, & RDI, 2026). Second, consideration should be given to avoiding the concentration of technical control over the entire SPE in a single third party. This may be achieved by distributing critical functions across different components and, where appropriate, different providers, so that no single third party has technical control over the SPE as a whole. These two safeguards are complementary as vendor substitutability reduces dependency on a particular provider, while architectural distribution can reduce the concentration of effective control in any single third party. Such measures can strengthen the HDAB's effective control and the resilience of the SPE, including in situations involving service unavailability, maintenance, restrictions on auditing, or other circumstances affecting an individual provider (including even external pressures unrelated to the service itself, such as commercial interests or external coercion).

Given the current state of technological development and the widespread availability of scalable and cost-competitive computing capacity, cloud services are expected to become an especially attractive option for providing the infrastructure and tools required to carry out processing operations involving highly sensitive data[30].

Against this backdrop, a central challenge concerns the establishment of trust in the guarantees claimed and implemented by cloud service[31] providers operating SPEs. It is therefore worth mentioning, before continuing, a classification of cloud services can be the "public cloud" and the "private cloud" (as well as hybrid models)[32], as the implementation and control that can be exercised over each is key in the context discussed in this document.

Data holders, data access bodies and data users should be able to rely on verifiable assurances that technical, organizational and contractual safeguards are effectively in place and consistently

[29] Article 73(3) of the EHDS mandates that regular audits of secure processing environments shall be carried out, together with the adoption of corrective measures to address any identified shortcomings, risks or vulnerabilities.

[30] The significance of cloud computing in relation to data protection challenges is further underscored by the fact that the first two transnational GDPR Codes of Conduct adopted at EU level both concern cloud computing processing activities; see EU Cloud CoC (https://eucoc.cloud/en/home) and CISPE CoC (https://www.cispe.cloud/code-of-conduct/)

[31] See Article 6(30) of the Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555) (hereinafter NIS2) for the definition of "cloud computing service", an equivalent term for "cloud service".

[32] See Recital (33) of NIS2.

enforced. This requires transparency regarding system architecture and security controls, robust contractual commitments, clear allocation of responsibilities, and the availability of independent audits. Trust is therefore not based solely on contractual promises, but on demonstrable compliance, continuous oversight and the ability to detect, prevent and remedy deviations from agreed safeguards. In particular, the decision to entrust the operation of a SPE to a third-party cloud service provider, rather than to a research institution or public body itself, calls for careful justification. Ensuring that "doing the right thing" prevails over merely "doing what is efficient" therefore requires a conscious assessment of the third-party operator, coupled with robust legal, contractual and technical arrangements that effectively replicate, or compensate for, the trust traditionally placed in institutional research environments when SPE operations are delegated to external providers.

At the same time, the objectives and constraints inherent to SPEs may come into tension with the business models or operational characteristics of large cloud service providers, including those designated as gatekeepers[33], whose position of economic and technological power renders effective assurance particularly complex[34]. The asymmetry of information and bargaining power that characterises the relationship between such providers and their customers may limit the latter's ability to negotiate tailored safeguards or to obtain sufficient transparency regarding internal processes and technical architectures. Similarly, given the scale, opacity, and global reach of these providers' operations, it cannot be assured that supervisory authorities will be able to perform their oversight responsibilities effectively and without undue impediment.

Additionally, a non-exhaustive list of relevant characteristics of a third-party service provider, whether categorised as a gatekeeper or not, that may increase the impact of risks to data protection and should be considered when analysing such risks includes the following:

- The type of services to be contracted (e.g. infrastructure, tools, scalability services, etc.).
- The type of processing activities implemented (identity management, data users management, etc.).
- The extent to which the HDAB retains full and effective control over the relevant processing operations.
- Limitations on the HDAB's ability to exercise effective auditing/oversight.
- Subjection to non-EU regulations and intelligence services.
- Whether international personal data transfers are in place.
- The complexity of investigating data breaches or verifying compliance with applicable legislation, including the GDPR.
- The use of data from different sources in the cloud and the associated risks of data linkage.
- Dominant market position.
- Possible discontinuity of services.

[33] See Articles 2(1) and 3 of the Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R1925).

[34] See for example The Guardian "Amazon Web Services outage shows internet users 'at mercy' of too few providers, experts say" [20 October 2025] https://www.theguardian.com/technology/2025/oct/20/amazon-web-services-aws-outage-hits-dozens-websites-apps

- Vendor lock-in or difficulties in migrating to an alternative provider.
- The resilience and availability of the cloud service provider.
- The possibility of access to cryptographic or pseudonymisation keys.
- The possibility of access to users' authentication information (including passwords).
- The high level of privileges or power held by the third-party service provider.

4. International transfers

Measures should be established to ensure that transfers to third countries do not take place unless it is ensured that appropriate safeguards and conditions, in accordance with the GDPR, are effectively implemented. In particular, Article 87(2) of the EHDS stipulates that personal electronic health data "*may be stored and processed in a third country, or a territory or one or more specified sectors within that third country, where such country, territory or sector is covered by an adequacy decision adopted pursuant to Article 45 of Regulation (EU) 2016/679*".

However, compliance with these requirements does not, in itself, necessarily ensure digital sovereignty or effective control over the data and the processing environment. Even where processing in a non-EEA country is covered by an adequacy decision, the involvement of entities or infrastructure subject to a non-EEA jurisdiction may raise additional considerations regarding such control. Therefore, the fulfilment of the GDPR requirements for international transfers and the preservation of effective control over the SPE should be considered as related but distinct considerations.

Consequently, the location and oversight of the hosting of the SPE, as well as the tools enabled for working within the SPE, must be contractually guaranteed in addition to all the topics addressed in the section "II.B.3. Third parties and the SPE implementation". Additionally, responsibilities in the event of a personal data breach (whether due to unauthorized access or the unavailability of the SPE or any of its tools[35]) must also be clearly defined.

5. Facilitating the exercise of data subjects' rights

The SPE should provide appropriate organisational and technical mechanisms to facilitate the exercise of data subjects' rights in accordance with the applicable data protection framework. The implementation of such mechanisms should rely on the basis that processing of data for secondary use may rely on legal bases other than consent, such as compliance with a legal obligation or the performance of a task carried out in the public interest. Depending on the applicable legal basis, the nature of the processing and any applicable restrictions or derogations, the SPE should effectively support, where applicable, requests concerning access, rectification, erasure, restriction of processing, objection and other relevant data subject rights. This may include dedicated interfaces for submitting and tracking requests, mechanisms for verifying/assessing the relevant requests, as well as procedures for implementing the corresponding actions, including where data have already been incorporated into derived datasets or analytical outputs. Where a right is restricted or does not apply under the applicable legal framework, the relevant procedure should provide for the appropriate assessment and communication of the applicable grounds.

[35] AEPD blog's post: "Operational sovereignty in the processing of personal data" [Feb 2026] (https://www.aepd.es/en/press-and-communication/blog/operational-sovereignty-in-the-precessing-of-personal-data)

6. Privacy by Design and by Default

Beyond the health sector, SPEs should be governed by robust governance frameworks that embed the principles of data protection by design and by default, as enshrined in Article 25 GDPR. In this context, the conceptual distinction between "data sharing" and "data access" becomes particularly relevant. While data sharing traditionally implies the transfer of datasets to data users, data access (especially as explicitly differentiated in DGA), emphasizes controlled reuse without loss of control by the data holder[36]. This distinction is especially relevant for the reuse of certain categories of protected or sensitive data held by public sector bodies, as it underpins trust, transparency and the effective exercise of data subject rights, which are central objectives of the Union's data governance framework[37]. From a data protection perspective, SPEs must operationalize key GDPR principles such as purpose limitation, data minimization, as well as integrity and confidentiality, from the design and by default[38].

EHDS mandates compliance with the GDPR for both primary and secondary uses of data[39], with particular emphasis on processing activities conducted within a SPE[40]. Article 52(2) to (5) of EHDS acknowledge that a formal fulfilment of the requirements of Article 73 of EHDS could be not enough for any electronic health data containing content or information protected by intellectual property rights or trade secrets. Article 52(2) lays down that could be "*parts of the datasets are concerned and justify the need for the specific protection of the data*", extending beyond personal data to include other sensitive data.

Therefore, even in the case of a SPE that fulfils requirements of Article 73 of EHDS, the HDAB shall deal with the fact that several data sets need special protection:

- That such protection shall be selected to deal with threats that would rise from various points of view: trade secrets, intellectual property and personal data protection.
- That protection measures could be legal, organizational and technical. That the risks should be assessed from such different points of view.
- And, finally, the assessment could lay down that the processing entails a serious and unmitigable risk of infringing intellectual property rights or trade secrets, the access to the data shall be refused.

It is important to emphasise the significance of this issue. For example, one potential secondary use could involve developing and implementing public health policies through the processing of personal data. Depending on the risks associated with such policies, such as those arising during a pandemic, availability and resilience must be ensured (as required by Article 32 of the GDPR) against physical, digital, or legal threats. In this case, an availability issue could arise, for instance, from a power supply failure, in which case the necessary measures would need to be implemented. However, another potential availability risk could stem from legal restrictions on use, such as those related to trade secrets, resulting from an incorrect implementation of the safeguards that the SPE must establish regarding trade secrets and intellectual property rights.

---

[36] It is also noteworthy that this concept of granting access to data without transferring it is explicitly reflected in another key piece of European legislation, namely the Artificial Intelligence Act. Recital (69) of the AI Act emphasizes that, in addition to ensuring compliance with data protection requirements throughout the entire lifecycle of an AI system, particular attention should be paid to technological approaches that avoid the transmission of data. Specifically, the recital highlights "*the use of technology that permits algorithms to be brought to the data and allows training of AI systems without the transmission between parties or copying of the raw or structured data themselves*", thereby reinforcing the relevance of access-based models that preserve data control while enabling innovation.

[37] Recital (5) of DGA.

[38] Article 73(2) of EHDS.

[39] Article 1 and Recital (5) of EHDS

[40] Recital (77) of EHDS

For this reason, HDABs must pay particular attention to ensuring that the required safeguards are appropriately implemented by design.

As it is described in previous section, a SPE shall be considered as an infrastructure that facilitate responsible data access and reuse, so as to ensure fulfillment of the personal data protection requirements. Therefore, the technical challenges to implementing such a SPE, from a data protection perspective, are tightly linked to meeting the strict conditions of its definition purs. to the Article 2 of the DGA, as well as of the Article 73 of the EHDS Regulation.

However, there is still no common understanding (let alone standardization) regarding how a SPE should be implemented in practice. Some elements that have been used towards implementing a SPE are known[41] and they all put emphasis on the fact that access to the data, as well as the export of data, are tightly controlled[42].

First, SPE shall be built on **zero-trust security principles**, where no user, device, application, or workload is trusted by default, regardless of whether it operates inside or outside the network perimeter (NIST, Zero-trust architecture, 2020), This is due to the fact that zero-trust architectures strengthen resilience against increasingly sophisticated and AI-accelerated cyber threats (ENISA, ENISA's view on Cybersecurity in the Frontier AI Era, 2026) This approach includes continuous identity verification[43], least-privilege access, strong authentication and continuous monitoring to limit lateral movements.

To this end, it is important to point out that implementing a **SPE is not only a matter of security applied to data protection**; it shall also be ensured that **all data protection principles** such as, e.g., data minimization and purpose limitation **are effectively in place**. From a data protection engineering perspective, a SPE should address both the protection of the data entering the processing environment (*input privacy*) and the protection of individuals against identification or singling out from the results released by the environment (*output privacy*) (ENISA, Engineering Personal Data Sharing, 2024). In fact, these principles should be present in all phases of the processing. In case of a HDAB under the EHDS that is to implement a SPE for the processing of electronic health data (such as the receiving, combination, preparation and compiling of necessary requested data from health data holders, as well as the pseudonymisation or anonymisation of the data), in order to provide access to strictly authorized data users, the HDAB should consider from the design stage of the SPE, and obviously long before any processing of personal data begins, if there are data protection engineering techniques that could be used as enablers to ensure that the HDAB can fully support the desired tasks without having access to the original health data. If this is the case, then it becomes evident that the SPE needs to be implemented accordingly, since by these means it will be ensured that the aforementioned data protection principles are satisfied.

a) Application of the precautionary principle by design

Given the specific characteristics of SPEs, the novelty of their use and the purpose for which they are implemented (namely, to facilitate the processing of particularly sensitive data) as well as the risks that can be identified in relation to the rights and freedoms arising from such processing,

[41] See https://healthycloud.eu/workshop-elements-of-secure-processing-environments/

[42] The importance of this matter is further illustrated by the work of the EU-funded TEHDAS2 Joint Action (https://tehdas.eu/project/), which has very recently developed common guidelines and technical specifications to support the harmonised implementation of the EHDS, including technical specifications defining core functional and security requirements for SPEs and providing a common framework for their implementation across Member States.

[43] This is regardless of whether access is granted for a specific period (subject to renewal) to a researcher or a research institution, as, in any case, the identity of the person accessing the system must be verified at all times.

it is worth taking a moment to reflect on applying the precautionary principle[44] by design. This approach is described in this report as an important methodological consideration and should not be understood as a specific regulatory requirement deriving directly from DGA, EHDS, or GDPR.

Therefore, an initial task is to identify cases involving similar infrastructure that have faced critical situations and to analyse them retrospectively in order to anticipate such situations. Some examples might include:

- Cases of service unavailability arising from the detection of potential breaches of EU law (whether through internal audits[45] or even through innovative technologies that expose vulnerabilities in the service). In such cases, a response plan must be in place, tailored to the criticality of the situations that may arise; it may even be necessary to have the option of accessing data via another entirely independent SPE (whether another infrastructure or another operator) so as to ensure service continuity.

- Cases in which a data user may extract detailed information from tables, models or statistics which, directly or indirectly, and reveal confidential information (e.g. through tables with too granular attributes, coefficients that allow individual records to be inferred, models that are too specific, or maps with excessive spatial resolution). In such situations, reviewing the results before they are finally made available to the data user is crucial for identifying these issues and implementing anonymisation mechanisms before enabling the data user to download the data.

- Cases in which attempts are made to reconstruct individual information through inference attacks (e.g. by running the same query repeatedly, by comparing results with slight modifications to the queries, through successive models, etc., and even any of these via coordinated attempts between two different data users). This situation could lead to the implementation of a manual review before making the data available to the data user and checking their previous requests; or by imposing a limit on the number of queries a data user may make; or by imposing specific data disclosure obligations on data users.

- Cases of non-compliance by data users (e.g. misuse of credentials, account sharing, uploading unauthorised material or non-compliance with the terms of use). These situations could be minimised through more detailed monitoring of data users' activity, which could lead to temporarily or permanently revoking access and even notifying the research institution for which the data user works.

- Cases of cyber incidents that generally result in service unavailability and may be caused, for example, by ransomware, network failures, or infrastructure vulnerabilities. In such cases, the implementation of cybersecurity measures is a fundamental step.

- Cases where AI models capable of detecting system vulnerabilities are executed in controlled

---

[44] In its "Communication from the Commission on the precautionary principle" (COM(2000)1 final) [Feb 2000] (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52000DC0001), the European Commission stated that: "*Although the precautionary principle is not explicitly mentioned in the Treaty except in the environmental field, its scope is far wider and covers those specific circumstances where scientific evidence is insufficient, inconclusive or uncertain and there are indications through preliminary objective scientific evaluation that there are reasonable grounds for concern that the potentially dangerous effects on the environment, human, animal or plant health may be inconsistent with the chosen level of protection*". In this regard, the EDPS has highlighted the appropriateness of applying the precautionary principle as a preventive measure in the case of data processing operations with a significant impact or where there is uncertainty as to what that impact might be (see "EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data" [19 Dec 2019] https://www.edps.europa.eu/sites/default/files/publication/19-12-19_edps_proportionality_guidelines_en.pdf).

[45] See for example The Guardian "Office for National Statistics has 'deep-seated' problems and needs an overhaul" [26 June 2025] https://www.theguardian.com/uk-news/2025/jun/26/review-calls-for-10m-overhaul-of-the-office-for-national-statistics

environments, potentially compromising the integrity of the infrastructure and implemented safeguards[46], which may result in significant security breaches with an impact on data protection.

b) Five safes framework

The Five Safes framework[47] (Ritchie, 2017) establishes a comprehensive approach that spans the design and planning of data-driven solutions. It is built on a layered protection model with five "control dimensions", known as the Five Safes, where each dimension must be analysed collectively. By addressing a simple yet critical question for each layer, the framework enables the development of a structured and systematic methodology. A key strength of this approach is that multiple layers must fail simultaneously for a real data breach to occur, thereby mitigating potential impact.

Safe projects	Is this use of the data appropriate?	Managerial controls
Safe people	Can the researchers be trusted to use it in an appropriate manner?	
Safe settings	Does the access facility limit unauthorised use?	
Safe data	Is there a disclosure risk in the data itself?	Statistical controls
Safe outputs	Are the statistical results non-disclosive?	

Figure 1: The five control dimensions of the Five Safes framework and the questions they raise (Ritchie, 2017).

This approach is then combined with the risk assessment methodology proposed in the following section, including a brief example in the use case described in section "IV. A use-case scenario".

7. Data protection risks management

In defining the main management processes that implement a governance model, risk management plays a key role. Risk management involves the prior identification of threats, followed by the assessment of their inherent risk levels for the rights and freedoms of natural persons, as well as the selection of risk management strategies based on organizational, legal, and technical measures.

In relation to the risks management, the obligation to conduct a Data Protection Impact Assessment (DPIA)[48] pursuant to Article 35 of the GDPR should be stressed. DPIAs enable data controllers to systematically identify and assess risks associated with the processing of personal data and to inform decisions regarding the implementation of appropriate technical and organizational safeguards based on a risk-based approach. Given that SPEs are typically intended for high-risk processing activities[49], the performance of a DPIA is generally required.

On the basis of DPIA outcomes, entities acting as data controllers for processing operations carried out within a SPE are required to select and implement suitable data protection engineering techniques before the processing takes place. Measures such as data minimization, anonymization, encryption of data at rest, in transit and, where technically feasible, in use, as well as strict access controls must be carefully assessed in terms of their effective implementation, with the aim of

[46] See Hugging Face "Anatomy of a Frontier Lab Agent Intrusion: A Technical Timeline of the July 2026 Incident" [27 July 2026] https://huggingface.co/blog/agent-intrusion-technical-timeline

[47] Official website of the Five Safes framework: https://fivesafes.org/

[48] Recital (15) of DGA.

[49] Article 29 Data Protection Working Party. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. WP 248 rev.01. Adopted on 4 April 2017. As last Revised and Adopted on 4 October 2017 (https://ec.europa.eu/newsroom/article29/items/611236)

prioritizing data protection while preserving the utility of data for the intended processing purposes. Moreover, appropriate measures are needed to facilitate the exercise of the data subjects' rights. The selection and deployment of such measures must be justified in light of the severity and likelihood of the identified risks.

Within the framework of the EHDS, SPEs should address threats related to data protection and privacy – apart from trade and statistical secrets, intellectual and industrial property, national security or other national requirements. Risks management for these requirements should not be conducted independently. Provided that a single governance framework (with specific characteristics) is essential, there should also be a unified risks management approach that integrates all requirements. Otherwise, the resulting measures may be ineffective, inefficient, not ensuring the fulfilment to the data protection principles.

In light of the above, and within the scope of this guidance document, this section identifies specific characteristics of SPEs and relevant risk factors that should be taken into account when identifying and managing data protection and privacy risks in each specific case. Managing privacy risks includes assessing the level of risk and identifying measures to mitigate the initial risk

Therefore, the following lists a number of SPE-specific risk factors that should be taken into consideration.

- Large-scale data processing[50]. The large volume of data processed, combined with currently available techniques on the market, may reduce the effectiveness of anonymisation mechanisms, thereby increasing the likelihood of re-identification.
- Specific characteristics of the data processed. The particular nature and sensitivity of the data to be processed may entail a higher potential impact on data subjects, depending on the categories of data involved.
- Inference of unexpected personal data. There is a possibility of inferring new personal data that were not foreseen within the scope of the investigation that justifies access to the personal data.
- The specific characteristics of users who wish to access this data. In each specific context of a SPE's implementation, the type of users expected to access the data must be assessed due to the potential impact on the level of risk associated with the processing, as well as other relevant data protection considerations, such as potential data transfers to third countries.
- Unlawful of unauthorised access to personal data. This is related with the possibility of access to personal data without proper authorisation or in violation of applicable rules.
- Massive data breaches[51]. In case of large-scale personal data breaches, significant consequences for data subjects may potentially occur.

In addition, a set of high-level risk factors has been identified and should also be taken into consideration:

- Changes in the legal framework. Developments relating to, e.g., international data transfers, may have a significant impact on infrastructures implementing data spaces.

[50] Article 29 Data Protection Working Party. Guidelines on Data Protection Officers ('DPOs') (wp243rev.01). 5 April 2017. Pages 7-8. https://ec.europa.eu/newsroom/article29/items/612048

[51] AEPD. "Guidelines to manage data breach risk in public sector bodies massive data communications" [mar 2023] (https://www.aepd.es/documento/guidelines-manage-data-breach-risk-public-sector-massive-data-communications.pdf)

- International tensions and geopolitical developments. Conflicts such as the war in Ukraine, including disruptions to services provided by US data companies in certain jurisdictions, or the recent war in Middle East, where large-scale data breaches affecting genetic databases have been reported, illustrate broader systemic risks to data protection.
- Disruptive technologies. The emergence of disruptive technologies, such as quantum computing (ENISA, Post-Quantum Cryptography: Current state and quantum mitigation, 2021) and strategies like HNDL[52], may undermine existing technical and organisational safeguards.
- Frontier AI models pose a growing cybersecurity and privacy threat by dramatically accelerating the speed and sophistication of attacks, compressing the time from vulnerability discovery to exploitation and challenging traditional defense capabilities (ENISA, ENISA's view on Cybersecurity in the Frontier AI Era, 2026).
- The possibility of becoming locked into providers based in third countries[53] in critical sectors, such as healthcare, may have an impact on the EU's welfare model, as well as on economic and even security aspects.
- Contextual crisis. Historical precedents, such as the Balkan wars, and geopolitical instability highlight the risk of potential breakdowns of the rule of law, which could have severe consequences for data protection and fundamental rights.

As outlined in Recitals (20) and (4) of the DGA, personal data could be inextricably linked to non-personal data that might include data protected by trade secrets or intellectual property rights. Consequently, any threat to datasets, whether arising from trade secrets, intellectual property concerns, or even national security risks tied to the sensitivity of the data being processed, can directly pose threats to data protection. These risks must therefore be holistically considered when conducting a data protection risk assessment. In fact, the corresponding risk assessment should reflect the nature, scale and sensitivity of the data concerned and should not be limited to conventional or low-capability threat actors. In particular, based on the context and the relevant risks, the threat model may need to consider sophisticated and well-resourced actors, potentially including state-level actors and intelligence services. Especially in cases that such threats are considered as reasonably foreseeable, any legal and contractual safeguards should be necessarily complemented by robust technical measures.

A specific exercise for analysing privacy risks should be carried out for each particular implementation of a SPE, taking into account the authorised use cases. All identified data protection risks must also be analysed in terms of their derived impact on other fundamental rights and freedoms.

All these considerations set out here – quite apart from the fact that there may be a number of other specific circumstances to take into account in each case – could even lead to the need to implement different SPEs under the control of the HDAB, depending on the type of users or the type of projects to be carried out, or other relevant circumstances.

All identified risks require the implementation of appropriate measures to reduce the level of risk to personal data protection. In accordance with data protection principles, such measures should aim to ensure fairness, unlinkability, transparency, and intervenability, alongside (cyber)security objectives such as confidentiality, integrity, availability, and resilience.

---

[52] Harvest Now, Decrypt Later (https://en.wikipedia.org/wiki/Harvest_now,_decrypt_later)

[53] See "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on European Tech Sovereignty, accompanied by an EU Open Source Strategy" (COM(2026) 503 final) (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52026DC0503)

A risk assessment for each case can be carried out based on the Privacy Threats Modelling LIINE4DU methodology (AEPD, Technical note: An Introduction to LIINE4DU 1.0: A New Privacy & Data Protection Threat Modelling Framework, 2024), which is built on a model of privacy threats categorised into the following ten threat categories:

- Linking: This threat involves associating different data items or data subject's actions to learn more about a data subject or group.
- Identifying: This threat involves learning the identity of a data subject directly (through the processing of identifiable information or leaks, for example) or indirectly (through deduction or inference, for example).
- Inaccuracy: This threat involves using obsolete, wrong, incomplete, biased or low-quality data that may lead to incorrect decisions or actions, potentially causing inconvenience or even harm to the data subject.
- Non-repudiation: This threat involves the ability to attribute a claim to the data subject (something they know, they are, they do, etc.) when this implies an impact on their fundamental rights and freedoms.
- Exclusion: This threat involves unintentionally or deliberately failing to adequately serve a data subject, hindering their participation or involvement in physical or digital life.
- Detecting: This threat involves deducing the existence of data items or data subject's actions through observation.
- Data Breach: This threat involves destruction, loss, alteration, unauthorised disclosure of, or access to, personal data by mistakes, malicious insiders or cyberattacks.
- Deception: This threat involves intentionally attempting to influence, coerce or manipulate the data subject into making unintended, unwilling and potentially harmful decisions, often against their best interests.
- Data Disclosure: This threat involves excessively collecting, storing, processing, or sharing/ transferring personal data.
- Unawareness and Unintervenability: This threat involves insufficiently demonstrating compliance or insufficiently informing, involving, or empowering data subjects in the processing of their personal data.

Finally, it should be emphasised that compliance with the GDPR is required irrespective of the level of risk associated with a given processing activity. In the context of the EHDS, however, processing for secondary purposes typically involves the large-scale processing of special categories of personal data. Consequently, pursuant to Article 35(3)(b) GDPR, the conduct of a Data Protection Impact Assessment (DPIA) is mandatory.

Overall, properly embedding data protection principles into data practices can help mitigating the risks of data misuse while creating the conditions for responsible innovation, collaboration, and value creation, as well as foster trust for the individuals (IDGDPT Berlin Group, 2024).

III. IMPLEMENTATION CONSIDERATIONS AND MEASURES

On the basis of the previous analysis, a SPE shall enable secure, privacy-friendly processing of personal data within a legally and technically robust framework, thus going far beyond a typical secure framework. Although a risk-based approach, depending on the specific context, shall be adopted when deciding how a specific data process will be implemented within a framework of a SPE, it must always be taken into account that the processing at issue should be considered as high-risk in terms of the impact for the rights and freedoms of individuals. This in turn necessitates some concrete requirements that shall be set as minimum, expected to be always in place. These requirements stem from the definition of the SPE in conjunction with the relevant (expected) applications of SPEs according to the existing legal framework as well as with established well-known requirements in the context of security and privacy risk management frameworks (see, e.g., (NIST, Security and Privacy Controls for Information Systems and Organizations, NIST SP 800-53 Rev. 5, 2020)).

A. Measures that shall be implemented

In this sub-section the aim is to set out those measures that could be regarded as establishing a "lower threshold"; therefore, fulfillment of these requirements is necessary but not necessarily adequate. In other words, the measures included in this catalogue reflect the minimum level of protection measures expected for the operation of a SPE, taking into account the security and data protection by design and by default obligations applicable to its role. Their inclusion should not, however, be understood as implying that each individual measure is prescribed in identical or explicit terms by a specific legal provision. Rather, the measures translate the applicable requirements into concrete safeguards that should be appropriately implemented. Furthermore, the list set out here describes the measures in broadly general terms, requiring, in each specific case, appropriate implementation in line with the particular circumstances of that case. These measures are presented in a technologically neutral manner, although some illustrative examples are provided for the sake of clarity.

The measures proposed here include both those relating to processing operations associated with the functioning of the SPE itself, and those directly related to the processing supported by this infrastructure; in many cases, these measures will serve both purposes, given that, for example, identity management, access controls and access logs are operations present in both types of processing, albeit to varying degrees.

1. Governance and accountability

1. Policy development and enforcement.
2. Opt-out mechanism. In the case of processing health data for secondary use, mechanisms shall be implemented to exercise the right to opt-out, as well as to reverse it.
3. Consent management. In cases where the legal basis for processing is consent, mechanisms shall be implemented to enable the withdrawal of consent at any time.
4. Mechanisms shall be implemented to ensure the traceability of data and datasets flows in order to guarantee the effectiveness of the exercise of data subjects' rights.
5. Establish a documented risk-based approach for determining the specific security controls and processes that shall be implemented.

6. Implementation of processes for the ethical and scientific assessment of the project through which the data user wishes to access the SPE, including justification for access to non-anonymised personal data[54] where applicable, an assessment of necessity and proportionality, and a GDPR compliance review, including DPIA.

7. Well-established effective procedures for managing user access and relevant responsibilities. Clear criteria[55] for granting access permissions, so that data users are not granted unlimited access. Permissions should be granted following a comprehensive review process.

8. Implementation of mechanisms to facilitate the review of the data included in a download request in order to assess the risk of re-identification in the dataset[56] and thus ensure that data users are only able to download non-personal data from the SPE.

9. Regulatory compliance mapping and continuous compliance verification through regular monitoring and auditing.

10. Compliance dashboard and metrics.

11. Rights exercise panels and interfaces.

12. Establish methods to ensure that EU data sovereignty rules are respected.

13. Provision of the necessary information from the SPE to the data controller in cases where the entity responsible of the SPE acts as processor.

14. Involvement of the Data Protection Officer (DPO), or data protection advisers, at all stages of the SPE (from planning and development through to its implementation, operation and even decommissioning).

2. Data management

15. Creation of catalogues[57] of available data and datasets, which shall be interoperable.

16. Data loss and unauthorised disclosure prevention (this may include Data Loss Prevention (DLP) technologies and/or equivalent technical or organisational measures).

17. Ensuring that only data that are adequate, relevant, and necessary for the authorised processing purposes are made available within the SPE (Data minimization).

18. Effective data de-identification (this is related with effective anonymization or possibly pseudonymisation techniques and may include measures like removal or transformation of direct identifiers, separation of identifiers from analytical variables, generalisation or suppression of attributes, aggregation of values, including infrequent values, or possibly other anonymisation or privacy-enhancing techniques).

19. Application of statistical and privacy enhancing technologies where possible.

[54] Article 67(2)(e) of EHDS.

[55] Article 68(12) of EHDS.

[56] This might involve reviewers checking, amongst other things, cells containing (or which may give rise to) outliers, too granular attributes, dangerous combinations of variables, coefficients that allow inference, overly detailed graphs, and models that could reveal individual information. If a risk is identified, the result shall be amended, aggregated, deleted, or simply not authorised for release.

[57] The identification and marking certain data and datasets is a case of particular interest for the data referred in Articles 51(4) and 52(2) of EHDS.

20. Implementation of mechanisms to ensure a limited availability period for data within the SPE.

21. Segregate data and datasets according to their sensitivity, purpose, access requirements, or other relevant risk characteristics, including the separate storage or processing of particularly sensitive data, as identified in the catalogue, where appropriate.

22. Data-at-Rest Encryption to prevent unauthorized access, ensuring confidentiality even if storage systems are compromised.

3. Identity Management and Access Control

23. Access must be limited to authorized individuals as defined by the relevant data permits which shall include the approved workflow for each case.

24. Prior verification of the identity of the data user (e.g., the research centre), as well as of the natural person acting on its behalf.

25. Principle of least privilege (PoLP). Access should be restricted to the minimum level necessary and granted only for the shortest duration needed to complete the task, ensuring that each data process is proportionate and purpose-limited.

26. Signing of confidentiality, data protection and acceptable use agreements between the entity responsible of providing the SPE and the data user[58].

27. Immediate revocation of access upon completion of the project.

28. Use of strong user identification and authentication methods (for example, via secure multi-factor authentication (MFA) schemes, certificates, etc.).

29. Regular review of access permissions.

4. Physical security

30. Access to SPE facilities must be physically controlled and verified (such as, e.g., through the use of security badges).

31. Secure, segregated premises with defined roles and access policies to prevent unauthorized physical access to devices and data.

32. Implementation of mechanisms to facilitate the deployment of necessary safeguards for each permitted access.

5. Network and communications security

33. Only non-personal or sufficiently anonymized data can be downloaded from the SPE.

34. Massive data flows should be automatically detected, audited and, if so, cancelled.

35. Data flows should be limited in the short and long term and subject to special process.

36. Incoming data should be routed through quarantine environments to verify its authenticity.

[58] As is laid down in Article 68(12) of EHDS "In order to reduce such costs and fees, the HDAB may also propose to the health data user to store the dataset in a storage system with reduced capabilities. Such reduced capabilities shall not affect the security of the processed dataset."

37. All data transfers into and within the SPE must occur securely, using state-of-the art cryptographic techniques (with sufficient key management processes) to protect against eavesdropping and unauthorized modification. This also entails strict network security measures (such as, e.g., network segmentation, traffic filtering).

6. System and applications security

38. Systems should be hardened (e.g., operating system hardening, application whitelisting).

39. Prevent unauthorized code execution or tampering.

40. Anti-Malware protection to detect, prevent, and remove malicious software like viruses and ransomware to safeguard systems and data.

41. Each processing environment (SPE instance) must be separated and isolated from different environments (to prevent unauthorized cross-access or data leakage between different applications/data sets).

42. Isolation of the SPE from the outside world to prevent data from being transferred in an uncontrolled manner (for example, by banning USB devices, blocking printers, disabling the shared clipboard, preventing synchronisation with cloud storage, and blocking direct access to the internet).

43. Patch management to regularly update software to fix vulnerabilities, improve functionality, and protect against cyber threats.

44. Implement Virtual Desktop Infrastructure (VDI), or other equivalent approaches, in order to facilitate a secure, controlled and monitored access to data.

7. Audit, Logging, Monitoring

45. Maintain comprehensive, auditable logs of all access and other operations, including, amongst others, logs of executed commands and logs of file accesses.

46. Logs should be monitored (user activity tracing and correlation), protected (i.e., through secure, tamper-proof logging mechanisms and comprehensive audit trails), and reported separately from core environments.

47. Log backups.

48. Real-time monitoring and alerting.

49. Security event dashboards which include anomaly detection and behavioural analytics to, in particular, detect unauthorised or abuse access.

50. Regular data protection audits and compliance monitoring must be conducted; in particular, for the health sector, audits on health data users to ensure compliance of the processing they carry out in the SPE[59], and internal and third-party audits on compliance of SPE with the defined standards, specifications and requirements[60].

[59] Pursuant to Article 73(1)(e) of EHDS.

[60] As referred to in Article 73(3) of EHDS.

8. Incident response, recovery and resilience

51. Incident detection and classification procedures.
52. Data breach response team and escalation paths.
53. Containment, eradication, and recovery procedures.
54. Backup and restoration mechanisms, including the creation of secure copies of critical data and regular testing of backup restoration procedures
55. Post-breach review and remediation procedures.
56. Communication and notification protocols.
57. Ensuring the availability and resilience of the SPE in line with the criticality of the service it supports. This could involve having a separate SPE running in parallel, either in terms of infrastructure and/or the operator.

9. Management of third parties

58. Incorporation of digital autonomy as a quality criterion in IT services by imposing specific and verifiable requirements and criteria, giving preference to solutions that meet the most stringent sovereignty requirements.
59. Provider risk assessment and due diligence. It shall include the assessment of the risk of vendor lock-in, and consequently adopting multi-vendor strategies and using open standards and interoperability as an explicit design principle in IT architecture.
60. Contractual security requirements (SLAs, permits, agreements, contracts).
61. Software Bill of Materials (SBOM) tracking.
62. Supplier tiering and critical vendor designation.
63. Data residency and cross-border transfer controls.

10. Organisational culture and training

64. Organisational culture and training
65. Role-specific training (developers, administrators, users).
66. Training on data protection and statistical confidentiality.
67. Incident reporting culture and channels.
68. Awareness campaigns highlighting the importance of applying the precautionary principle in all its aspects to the management of the SPE, as well as to all the processing operations it supports.
69. Promoting digital autonomy and technological sovereignty within the organisation.

B. Data protection engineering to implement a SPE

In the previous sub-section, we discussed specific measures to address relevant risks in the context of SPEs. However, as it is stated above, these may not be sufficient – despite their necessity. More precisely, when implementing a SPE, advanced cryptographic techniques and protocols that are particularly relevant to privacy-enhancing or privacy-preserving applications shall be taken into account; indeed, such tools can facilitate responsible data sharing and interaction in scenarios where, without them, trust may be insufficient (ENISA, Engineering Personal Data Sharing, 2024). These techniques inherently support the realization of the so-called secure computations, which, by definition, constitute a fundamental building block of a SPE.

We shall next briefly present, as indicative examples, specific cases of such advanced cryptographic techniques that provide data protection safeguards which fit well with the desired properties for a SPE. Of course, none of them should be considered as panacea, neither all of them are always possible or necessary (since, as we will see, each of them has its own limitations). However, since these techniques offer specific data protection benefits that go far beyond security, they should be necessarily taken into account towards implementing a SPE.

1. SPEs vs TEEs

First, it should be clarified from the beginning the SPE does not coincide with a Trusted Execution Environment (TEE), regardless the fact that, in practice, a TEE could be possibly used as a building block for a SPE. TEEs are typically considered as promising approaches to implement the so-called confidential computing to safeguard sensitive workloads even when running on untrusted cloud service providers. TEEs utilize specialized hardware within the Trusted Computing Base (TCB) (such as system-on-chips (SoCs) with memory management units (MMUs) and memory encryption engines (MEEs)) to establish a secure, isolated environment for executing sensitive code. By these means, they allow for secure execution of code by isolating themselves from the host system's operating system, kernel, and hypervisor. This isolated execution space aims to provide strong confidentiality and integrity guarantees, shielding data and processes from compromised system software and even from physical threats to the server hardware. Furthermore, TEEs incorporate a cryptographic root of trust (RoT) within the SoC, enabling remote attestation to verify both the hardware platform and the integrity of the TEE instance (Li, Yang, Chen, Yan, & Zhang, 2025). Therefore, in simple words, TEEs use a hardware root of trust to enable data processing with fine-grained access control and protection of the executed code, runtime state, and memory of cloud systems (Birrell, et al., 2018), (Sehgal, Bhatt, & Acken, 2020).

However, from a data protection point of view, a TEE has important limitations, mainly stemming from the fact that TEE internals are often closed-source and opaque, as they rely on hardware provided by specific vendors, thus yielding to reduced transparency; in fact, even remote attestation services may not be transparent. Other issues also exist, such as possible vulnerabilities to side-channel attacks and limitations due to constrained memory and storage. Moreover, TEEs in principle focus on security and not to other data protection principles. Concluding, on the basis of above, and taking into account the definition and the use of a SPE, TEEs by themselves shall not be considered as SPEs, although they may support the implementation of a SPE[61].

2. Homomorphic encryption

Traditional cryptography aims to transform the original data (i.e., the plaintext) into an obfuscated form (i.e., a ciphertext). The encrypted information looks like a random set of data and, thus, any operation amongst ciphertexts is meaningless. On the other side, a homomorphic encryption (HE) scheme additionally enables computations to be performed directly on ciphertexts, such that

[61] See, e.g., the Deliverable D4.3 'System Specfication and Arhitecture' from the JOCONDE (Joint On-demand COmputation with No Data Exchange) project (available in https://cros.ec.europa.eu/book-page/joconde)

the resulting ciphertext corresponds to the outcome of equivalent operations on the underlying plaintexts. This allows data to be processed in encrypted form without requiring decryption. There exist schemes that allow either homomorphic addition or multiplication operation, and there are also fully homomorphic encryption (FHE) schemes that allow both operations[62].

In the context of implementing a SPE, homomorphic encryption can serve as a suitable foundation when data users need to perform operations on numeric values. Such case studies could include, e.g., predicting medical device performance or patient monitoring for research purposes, which are based on vast amounts of numerical medical data. To this, implementing, e.g., linear regression is a typical approach and this may be performed over homomorphically encrypted values. By these means, no party gets access to the original numeric values – i.e., not only the data users, but neither the intermediary entity corresponding to the SPE provider. An illustrative figure is provided next[63].

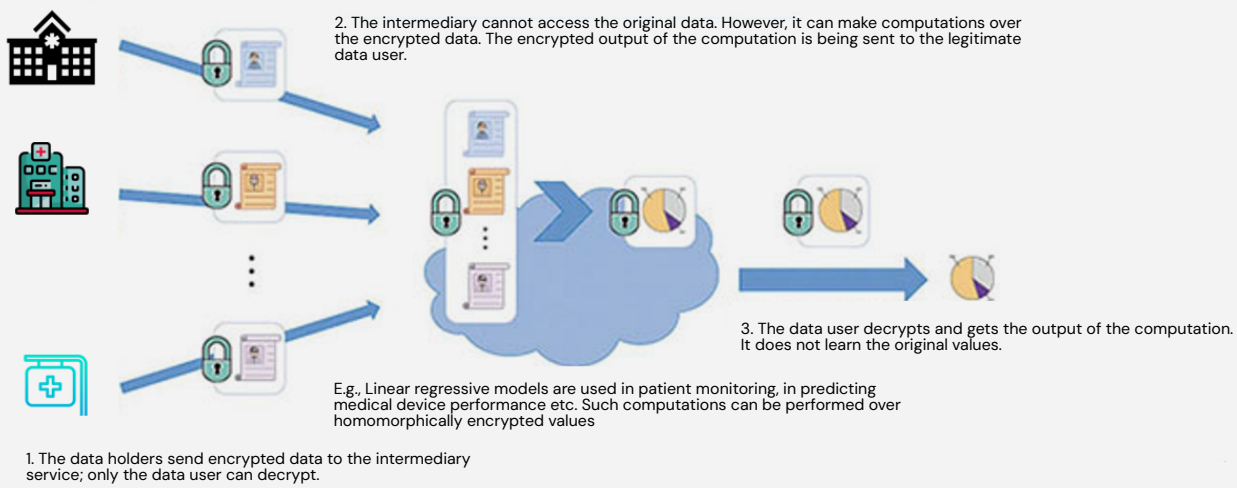


Figure 2: An example of homomorphic encryption towards implementing SPE in the health sector

As a last remark, although Fully Homomorphic Encryption (FHE) has long been regarded as a complex and resource-intensive functionality with significant practical limitations, recent advancements have demonstrated its viability, even in more demanding application scenarios.

3. Secure Multi-Party Computation

Secure Multi-Party Computation (SMPC) protocols are cryptographic techniques that enable multiple parties to jointly compute a function over their private inputs without revealing those inputs to one another. Intuitively, SMPC protocols allow parties to jointly obtain a permitted computation result without having to disclose their inputs to one another; each party can participate in the computation without gaining direct access to the other parties' underlying data. The information revealed to a party is therefore limited to the agreed output and any information that can legitimately be inferred from it.

A valuable feature of SMPC is its ability to distribute trust and control among multiple computing parties, thereby avoiding reliance on a single point of trust. Indeed, the computation requires the participation of multiple parties, while no single party has access to all the information needed to

[62] Some algorithms allow Boolean comparisons, like TFHE that stands for Torus Fully Homomorphic Encryption

[63] Note that the operations over encrypted data could be performed either by the intermediary or by the data users themselves (within the intermediary's environment): in any case though, no entity is able to get access to the original values

reconstruct the protected inputs. This form of shared control is an inherent characteristic of SMPC (although similar forms of distributed control may also be achieved through other technologies).

SMPC protocols could be based on building block technologies like oblivious transfer, garbled circuit, commitment scheme, zero-knowledge proof, homomorphic encryption and secret sharing (Zhou, et al., 2024)[64]. It is interesting to point out that SMPC protocols have been already considered to enable organizations to perform joint statistical computations without exchanging intelligible data[65].

4. Polymorphic encryption and pseudonymisation

Traditional cryptographic methods are based on the principle that each ciphertext corresponds to a unique decryption key. However, more advanced techniques relax this constraint to enable a different functionality: a ciphertext— that can be decrypted only by its creator—can be transformed (or re-encrypted) in such a way that only a specific, authorized recipient can decrypt it using their own key. This capability is a fundamental feature of what is known as polymorphic encryption (Verheul, Jacobs, Meijer, Hildebrandt, & Ruiter, 2016). In other words, through polymorphic encryption, data can be encrypted in such a way that there is no need to fix a priori who can decrypt the data (ENISA, Engineering Personal Data Sharing, 2024). The important property of polymorphic encryption is that the entity that performs this re-encryption does not have access to the original data – neither to (any) decryption key. Therefore, if such an entity is an intermediary within the framework of a SPE, then this intermediary manages to provide access only to legitimate users without having access to the original data.

However, polymorphic encryption should be considered alongside pseudonymisation. As described in (Verheul, Jacobs, Meijer, Hildebrandt, & Ruiter, 2016), the entity responsible for re-encryption also carries out pseudonymisation—i.e., through replacing individuals' identifiers with pseudonyms that appear random. This process is applied directly to the encrypted data (so this entity still does not get access to the original data), ensuring that when an authorized user decrypts it, they receive pseudonymised information. Furthermore, if the same encrypted dataset is re-encrypted multiple times for different users, the resulting pseudonyms are distinct and unlinkable across users.

The above properties are shown in the following figure.

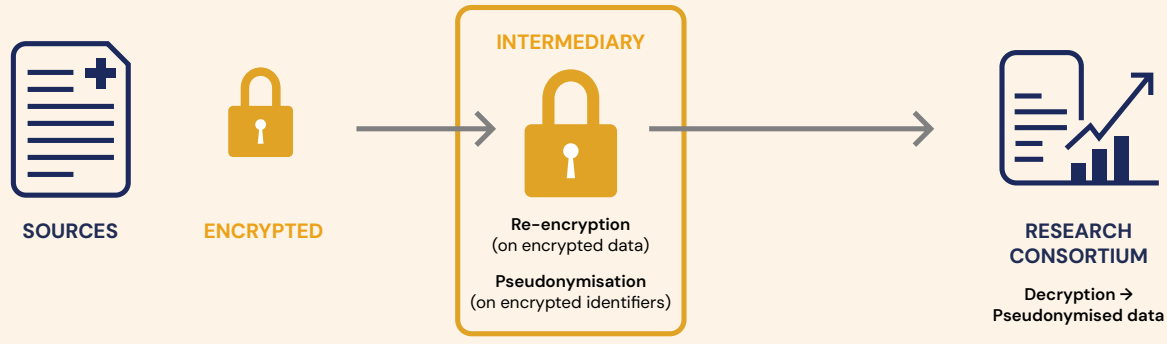


Figure 3: A simplified diagram on the polymophic encryption and pseudonymisation

[64] See also the D2.1 'Technology Survey and Analysis' report from the JOCONDE (Joint On-demand COmputation with No Data Exchange) project for a thorough analysis of the SMPC landscape (available in https://cros.ec.europa.eu/book-page/joconde).

[65] See, e.g., JOCONDE (Joint On-demand COmputation with No Data Exchange) project where it is explicitly stated that Eurostat considers this possibility https://cros.ec.europa.eu/book-page/joconde; Ricciato, F. 2024, Steps Toward a Shared Infrastructure for Multi-Party Secure Private Computing in Official Statistics, SageJournals, https://doi.org/10.1177/0282423X241235259

Polymorphic encryption and pseudonymisation has been already used in the context of a Large-Scale Parkinson's Disease Study (van Gastel, Jacobs, & Popma, 2021). The aforementioned properties illustrate its importance in terms of providing safeguards that are essential for a SPE.

It should be stressed that, in such a setting, pseudonymisation relies on replacing original identifiers with pseudonyms. However, depending on the dataset's structure and content, this measure alone may be inadequate. For instance, re-identification may be still possible by the data user in case that the dataset contains quasi-identifiers that allow for circumventing pseudonymisation (Samarati, 2001). This further underscores the importance of applying a thorough, risk-based approach when implementing a SPE.

5. Oblivious pseudonymisation

A SPE provider shall ensure that legitimate users get access to data that cannot be attributed to a specific person. To this end, robust pseudonymisation techniques could be implemented – probable based on strong cryptographic algorithms. Typical pseudonymisation approaches necessitate that the entity that performs pseudonymisation has knowledge of the original identifier (ENISA, Pseudonymisation techniques and best practices, 2019), (EDPB, 2025). However, there exist techniques that are based, amongst others, on the cryptographic notions of oblivious PRFs (Pseudo-Random Functions) that allow to provide the so-called oblivious pseudonymisation-as-a-service (Lehmann, 2019), which suffices to ensure the following properties:

i. The pseudonymisation is outsourced to a central entity (i.e., a cloud provider as a gate keeper), being though fully oblivious: the service provider does not learn neither the sensitive information (including the original identifiers) not the pseudonyms it produces. The pseudonyms are actually PRF values.

ii. When data is stored at rest, they are pseudonymised in a fully unlinkable manner, whilst the original identifiers cannot be mathematically recovered through pseudonymisation reversal. Unlinkability is ensured by splitting the information about individuals into unlinkable tables.

iii. When certain subsets of data are needed for a legitimate data user, only then the linkage is established though a controlled and non-transitive join operation; i.e. only the legitimate data user will get these pseudonymous data, so as even if another data user asks for accessing the data, the correlation of these two different snapshots will be unlinkable.

iv. The join operator allows for creating, for any single individual, the same irreversible pseudonym (also "blindly", through an oblivious PRF).

With this approach, data are securely stored (in terms of hiding identities and not allowing singling out) at the HDAB before any access request; for each such request, and once access is granted, a proper join operation is "blindly" performed. Nobody gets access to the original data.

Of course, the above procedure focuses on properly pseudonymising the individuals' identifiers; obfuscation/masking though is still needed for quasi-identifiers (as in the case of polymorphic encryption).

6. Differential privacy

Differential privacy (Dwork, 2006) is a rigorous framework designed to protect individual privacy in data analysis by introducing carefully calibrated random noise to query outputs. In simple words, differential privacy weakens the relationship between an individual's presence in a dataset and the result of an analysis. i.e., observing the output should not allow an observer to determine with confidence whether a particular individual's data contributed to it. Thus, the output is intended to reveal information about the dataset or population as a whole, without materially increasing

what can be learned about any single individual. More formally, this ensures that the inclusion or exclusion of any single individual's data in the dataset has a negligible impact on the final result. The noise is statistically controlled to balance privacy and utility: it must be sufficient to mask individual contributions while preserving the overall accuracy of the aggregated data. This approach is particularly valuable in scenarios where sensitive data, such as medical records or financial information, is analyzed and, in fact, it may be an approach to implement the measure numbered 8) in the relevant catalogue in Section III. A. By quantifying privacy loss through parameters, differential privacy provides a measure of the risk of re-identification.

It should be pointed out though that the trade-off between privacy and utility should be carefully considered. Strict differential privacy guarantees may require (depending on the case) substantial amounts of noise, potentially reducing the utility of the resulting data. In practice, different variants and implementations of differential privacy may therefore provide different levels of protection.

7. Federated learning

Federated Learning (FL) (EDPS & AEPD, 2025) is a privacy-enhancing technology based on artificial intelligence, specifically machine learning. It enables multiple data sources to collaboratively train a shared model while keeping the data decentralised.

Instead of centralizing data in one location:

- Data remains on users' devices.
- A machine learning model is distributed to each device.
- Devices train the model locally.
- Only model updates (e.g., gradients or weights) are shared with a central server or collaboratively among devices.

Rather than sending raw data to a central server (if one exists), each source processes its own data locally and shares only the model updates. However, despite the privacy advantages of a FL approach, it should me mentioned that keeping the raw data local does not, by itself, guarantee their protection. Model updates may encode information about the data used for local training and, under certain conditions, may enable information about individual training records to be inferred or reconstructed, for example due to memorisation effects (see, e.g., the relevant discussion in (Ricciato, 2026) and the references therein). Therefore, model updates should not automatically be regarded as anonymous or non-sensitive information, and the privacy protection offered by FL should be assessed in light of the specific architecture, threat model and additional safeguards employed.

Finally, it is important to note that FL does not necessarily conflict with the requirement for central supervision of a SPE, provided that the federated architecture is designed such that the SPE operator retains centralised control and supervision over the overall processing workflow[66].

C. Mapping threats and measures

We next present a working framework for conducting a comprehensive analysis of the measures that should be implemented for data protection, based on the LIINEDU methodology combined with the Five Safe framework introduced in the previous section. This is presented schematically for

[66] This has been also considered in the relevant EU-funded project TEHDAS2 – see D7.4, available in https://tehdas.eu/wp-content/uploads/2026/06/d7.4-technical-specification-for-health-data-access-bodies-on-the-implementation-of-secure-processing-environments.pdf

practical use, and section "IV. A use-case scenario" includes, by way of example, a risk analysis of the threat posed by "Linking", together with a list of proposal of measures.

Threats to data protection	Measures that might lower the associated risks to data protection				
	Safe projects	Safe people	Safe settings	Safe data	Safe outputs
Linking					
Identifying					
Inaccuracy					
Non-repudiation					
Exclusion					
Detecting					
Data Breach					
Deception					
Data Disclosure					
Unawareness and Unintervenability					

Figure 4: Proposed scheme for identifying appropriate measures to minimise the risks arising from the identified threats to data protection

IV. A USE-CASE SCENARIO

Next, a use case scenario of a SPE is presented, relying on data protection engineering techniques.

A. Description of the scenario

A research consortium composed of several academic and public health institutions wants to investigate the relationship between allostatic load (a composite biomarker of chronic stress) and various demographic and socioeconomic variables (see, e.g. (Robertson T., 2016)). To this end, the study seeks data from multiple health and administrative data holders (e.g. hospitals, national health registries, statistical offices).

The consortium aims to perform linear regression analysis with the aim of describing the relationship between one outcome variable (in this case, the allostatic load, being the so-called dependent variable) and one or more exposure (or independent) variables.

In this specific use case, we assume as independent variables[67] the age, sex and area of residence (i.e., ZIP code) as well as the socioeconomic status (SES). Linear regression aims to compute a linear equation (i.e., the relevant coefficients) that describes effectively such a relationship.

In accordance with the provisions of the EHDS, the research consortium requests such data (which also include health data – i.e., a special category of personal data[68]) via a HDAB, which checks the inquiry and issues a data permit, which means that the consortium shall have access to relevant information via a SPE.

[67] They are also known as covariates in the regression analysis.

[68] Article 9 of GDPR.

B. Data protection risks analysis (related to linking)

The following sub-section analyses data protection risks using the previously introduced LIINE4DU methodology to identify appropriate measures for implementation in a SPE. This analysis focuses on facilitating the processing of the requested data while ensuring compliance with privacy requirements.

To avoid excessive document length and maintain flexibility (given that this is a brief introduction to the case without full contextual details) we provide an overview of linking threat analysis along with proposed mitigation measures. More precisely, with respect to the threat of linking, we state as requirement that the consortium must not access any information that could enable linking of individuals with external datasets, which in turn could yield identification of individuals. Indeed, although direct identifiers are not required for this use case, combinations such as "age-sex-ZIP-SES", when cross-referenced with the data holders' pool, may still allow re-identification in certain scenarios (see, e.g., (Samarati, 2001), (Sweeney, 2002)). Therefore, such information cannot be classified as anonymous.

Below are a number of preliminary considerations to bear in mind in order to mitigate the risks arising from the threat of linking, and consequently to identify and properly implement the necessary measures:

- Download restrictions within the SPE are insufficient to fully mitigate linking threats. The primary risk arises when users can group data within the environment, potentially associating different data items or user actions.
- Quasi-Identifiers: Variables such as age, sex, ZIP code/area of residence, and socioeconomic status (SES) are powerful quasi-identifiers. When the consortium links data from hospitals, registries, statistical offices, and administrative records, these variables (either individually or in combination) can single out individuals or very small subgroups.
- The consortium may derive linked group-level patterns for specific ZIP codes or SES strata, inadvertently revealing sensitive information about protected or vulnerable subgroups.
- Repeated regression runs, stratification, and iterative modeling can cumulatively aggregate subgroup-specific information over time, heightening linking risks, particularly when producing highly detailed outputs.

Following this preliminary analysis, an example is provided of some measures identified as most appropriate for this case from amongst those listed in the section "III.A. Measures that shall be implemented".

Threats to data protection	Measures[69] that might lower the associated risks to data protection				
	Safe projects Is this use of the data appropriate?	Safe people Can the researchers be trusted to use it in an appropriate manner?	Safe settings Does the access facility limit unauthorised use?	Safe data Is there a disclosure risk in the data itself?	Safe outputs Are the statistical results non-disclosive?
Linking (Associating different data items or data subject's actions to learn more about a data subject or group)	6), 7), 14)	25), 26), 64)	31), 32)	15), 16), 17) 18), 19), 20) 21), 22), 33)	8)

Figure 5: Example of measures to address data protection risks arising from Linking in the use case described.

[69] All numbers in this table refer to the list of all the measures set out above in section "III.A".

Amongst the above measures, the effective data de-identification (numbered 18) is of high importance with respect to mitigate the linking threat. The choice of the proper de-identification techniques shall occur taking into account the inherent characteristics of the process, in conjunction with the relevant risks for rights and freedoms of individuals. It may be the case that effective de-identification can be ensured through an advanced data protection engineering technique (as also implied by the measure numbered 19). This will be further analysed next.

C. Data protection engineering approach

The above analysis has not addressed the risks relating to linking arising from the management and maintenance of the SPE itself. In other words, similarly to the requirement for the research consortium, the HDAB or any of its processors shall not be able to link (or possibly identity) individuals. Hence, if the HDAB can fulfill its data sharing obligations without accessing the original data, this approach should be prioritised.

A data protection engineering technique that could be used to address the aforementioned challenges is the application of homomorphic encryption (HE) on the original personal data, so as to perform linear regression on encrypted data. Indeed, recalling the properties of HE described in section "III.B. Data protection engineering to implement a SPE", the data holders can homomorphically encrypt their data before submitting them to the HDAB, which in turn will be in place to perform linear regression without having access to the original data: the output of this analysis will be also encrypted, which will be accessed by (or shared to) the research consortium. Then, the research consortium will decrypt this outcome, thus getting the coefficients computed; the research consortium does not get access to personal data, neither can infer any personal information, whilst its research goals are effectively fulfilled.

D. The data protection engineering technique in detail

1. Step 1: Agreement and Setup

- The consortium submits a data access application to the HDAB, outlining the study design. The HDAB checks and validates the application, issuing a data permit with specific parameters, in accordance with what is required under EHDS secondary use purposes.

- This is the step that the HDAB decides on the data protection engineering technique that will be used – i.e., HE for this case. In case that HE is supported by a third party (e.g., a Privacy-Enhancing Technology (PET) provider), then this party is appropriately employed at this stage, providing the relevant cryptographic tools for keys setup and cryptographic operations; otherwise, the HDAB shall proceed with this setup.

2. Step 2: Cryptographic Keys Management

- The research consortium generates[70] a homomorphic encryption key pair:
  - Public key is securely shared with data holders (through the HDAB).
  - Private key is kept securely by the research consortium.

[70] The HDAB, probably with the assistance of a PET provider, should assist the research consortium for this step.

3. Step 3: Sending encrypting data to the HDAB

- Each data holder encrypts the requested data (i.e., allostatic load score, age, sex, ZIP code, SES indicators such as income quintile, education level etc.)[71] locally, using the consortium's public HE key and the corresponding HE algorithm.
- The encrypted datasets are sent to the SPE orchestrated by the HDAB.
  - Plaintext data never leaves the data holder. Additionally, neither the HDAB nor any other party that possibly supports HDAB can get access to the plaintext data or to the decryption key.

4. Step 4: Secure Computation via HDAB

- The consortium uploads to the SPE linear regression code that operates on encrypted data.
  - The HDAB shall check this input provided by the consortium (e.g., for possible malicious code).
- Computation is performed directly on the encrypted data (due to the HE), without ever decrypting it.

5. Step 5: Sharing results

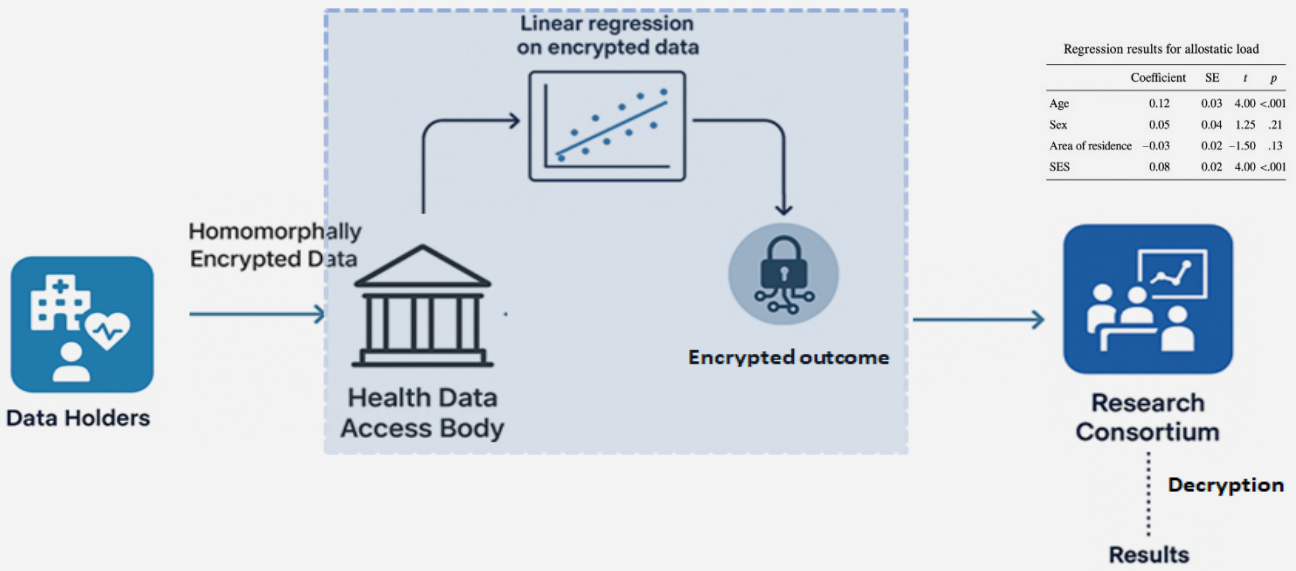
- The HDAB returns encrypted regression results (e.g., coefficients) to the research consortium. This takes place in a secure way, to ensure entity and data authentication.
- The consortium uses their private key to decrypt the results.
  - Alternatively, accessing to encrypted results and secure decrypting of them could be performed within the SPE, under a proper implementation that allows secure and private access to these data. By these means, the HDAB could verify that no personal data will be submitted to the research consortium.

6. Step 6: Analysis and Reporting

- The decrypted results are interpreted and reported.
- No individual is re-identifiable by any party.
- Only permitted secondary uses (e.g. scientific research) are possible.

Basic steps of the above process (namely, Steps 3 – 5) are shown in next Figure.

[71] These variables shall be first encoded appropriately, in order to subsequently feed the linear regression algorithm.



Regression results for allostatic load

	Coefficient	SE	t	p
Age	0.12	0.03	4.00	<.001
Sex	0.05	0.04	1.25	.21
Area of residence	−0.03	0.02	−1.50	.13
SES	0.08	0.02	4.00	<.001

Figure 6: Illustrating the use-case scenario

Although, in this use case, the computation is performed by the HDAB on behalf of the research consortium, rather than directly by the data users within the SPE, the model remains consistent with the general concept of a SPE as a mechanism for enabling secure access to and re-use of data. In this case, secure access is achieved through the controlled execution of the requested computation and the provision of the authorised output, without granting the data users access to the underlying data. In any case though, this data protection engineering technique could also be adapted to allow the research consortium itself to perform the computations within the SPE environment using homomorphic encryption.

By these means, neither the SPE provider nor the data user get access to any part of the original data; the computations are fully confidential, data remain always encrypted, neither the SPE nor the data user learn any information that allows direct or indirect identification of an individual or even inferring any information for a person, whilst the encryption algorithm also ensures the integrity of the data inside the SPE. Therefore, a proper implementation of this data protection engineering technique aims to directly address the threats related not only to linking, but also to identifying, non-repudiation, detecting, data breach and data disclosure. Moreover, this technique also contributes in alleviating threats like inaccuracy (since the data cannot be modified within the SPE without such a modification being detected), as well as deception and unawareness (since if the users are well-aware of the characteristics of the overall process, they will be no mistaken on how their rights are being respected neither they will be manipulated on their choices).

This data protection engineering approach also fits well with the 'Five Safes' approach. Indeed, this solution inherently addresses the disclosure risk in the data ('safe data'), whilst the statistical results are non-disclosive ('safe output'). Moreover, the homomorphic encryption in conjunction with proper key management ensures that unauthorised use is prevented ('safe settings'). Of course, provided that proper authentication methods are established for the researchers of this consortium (which is prerequisite for implementing this solution), in conjunction with the fact that the consortium does not get access to personal data as well as that there is a formal project approval and specification of the authorised purposes, data, users, processing activities, duration, and outputs, this approach is in line with the 'safe project' and 'safe people' principles.

More generally, this example illustrates that the safeguards provided by the SPE may be considered among the relevant factors in the overall balancing assessment, in conjunction with the nature and

sensitivity of the data, the purposes and interests pursued through the data re-use, including the advancement of research and innovation, and the risks to the rights and freedoms of data subjects.

Finally, it is important to note that the use of an advanced privacy enhancing technology (like, e.g., homomorphic encryption) does not, by itself, determine the respective roles of the parties under the GDPR. Where the HDAB acts as a processor rather than as a controller in relation to the processing carried out within the SPE, and the technical infrastructure is provided by a separate service provider, the latter may act as sub-processor, depending on the respective roles and responsibilities of the parties. In such a case, the requirements of Article 28(4) GDPR concerning the prior specific or general written authorisation of the controller for the engagement of another processor would also need to be taken into account.

V. FINAL REFLECTIONS

Secure processing environments are becoming a cornerstone for allowing secure data sharing in increasingly interconnected and data-driven ecosystems such as the European data spaces, as they *"provide the structured sources of trustworthy data"* and *"are central to building a single market for data"*[72]. As the cybersecurity landscape continues to evolve, driven by advances in artificial intelligence and the emergence of quantum computing, secure processing environments must therefore be designed with resilience, adaptability, and security by design as fundamental principles.

A comprehensive approach should combine robust technical safeguards with appropriate organisational measures, implemented through a risk-based methodology that reflects the high-risk nature of many processing operations. This includes the adoption of zero-trust architectures, where no user, device, or workload is implicitly trusted, and access is continuously verified based on identity, context, and least-privilege principles. To this end, continuous monitoring, strong authentication and access control mechanisms are essential elements of such an approach, ensuring that the SPE operates within an infrastructure that guarantees legal compliance and digital sovereignty for the providing entity, without relying on assurances from data users, whether they are private entities, public bodies, or individual researchers.

At the same time, security should be complemented by advanced data protection engineering techniques when needed, such as privacy enhancing encryption (e.g., homomoprhic encryption) and secure multi-party computations. These technologies enhance security while supporting compliance with data protection requirements and enabling trusted data sharing and collaborative processing.

SPEs are not solely data protection or security measures. Like many Privacy-Enhancing Technologies (PETs), they are dual-use technologies (AEPD, Data Spaces, sovereignty and privacy by design, 2023) that address a range of data access challenges arising from legal requirements, market demands, and other considerations. SPEs should be understood as data access enablers that serve the interests of diverse stakeholders, including industrial laboratories, research institutions, national security agencies, and operators of critical infrastructure.

Beyond data protection concerns, the appropriateness of SPE measures may also influence the availability of secondary use of health data. Consequently, a high degree of protection within SPEs is not merely a matter of safeguarding personal data. For instance, in exceptional circumstances (such as a global pandemic or other major public health emergencies) access to pharmaceutical or

[72] Communication from the Commission to the European Parliament and the Council. Data Union Strategy. Unlocking Data for AI (COM(2025) 835 final) [November 2025] (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52025DC0835)

laboratory data may be indispensable for protecting life and public health on a large scale. In such cases, a rigid, binary approach that automatically denies access may not be suitable.

Thus, SPEs must draw from requirements originating from multiple sources.

Within a SPE's governance framework, it is essential to include the role of a Data Protection Officer (DPO) or a data protection advisor. This individual should possess expertise in data protection regulations, understand the specifics of the processing activities involved, and be capable of identifying and implementing appropriate technical and organizational measures to ensure data protection by design and by default. Additionally, the DPO should oversee compliance and manage critical impacts and risks to the rights and freedoms of individuals, with a particular emphasis on ensuring that Data Protection Impact Assessments (DPIAs) are systematically conducted, adequately documented, and effectively integrated into the design and operation of processing activities. Given that each processing activity that relies on a SPE may entail distinct risk profiles depending on its context, nature, scope and purpose, DPIAs serve as the key mechanism for determining and justifying context-specific organisational and technical safeguards rather than relying on uniform or generic controls.

VI. REFERENCES

ACM, AFM, AP, DNB, & RDI. (2026). *Towards digital autonomy - Increased control over digital dependencies*. Authority for Consumers and Markets (ACM). Retrieved from https://www.acm.nl/system/files/documents/towards-digital-autonomy.pdf

AEPD. (2023). *Approach to Data Spaces from GDPR Perspective*. Retrieved from https://www.aepd.es/documento/approach-to-data-spaces-from-gdpr-perspective.pdf

AEPD. (2023, September). Data Spaces, sovereignty and privacy by design. Retrieved from https://www.aepd.es/en/prensa-y-comunicacion/blog/data-spaces-sovereignty-and-privacy-by-design

AEPD. (2024). *Technical note: An Introduction to LIINE4DU 1.0: A New Privacy & Data Protection Threat Modelling Framework*. Retrieved from AEPD (2024). "Technical note: An Introduction to LIINE4DU 1.0: A Nhttps://www.aepd.es/guides/technical-note-introduction-to-liine4du-1-0.pdf

Birrell, E., Gjerdrum, A., R., v. R., Johansen, D., Johansen, B., & Schneider, F. (2018). SGX enforcement of use-based privacy. *Proc. 2018 Workshop Privacy Electronic Society – WPES.18*, (pp. 155–167.).

Dwork, C. (2006). Differential Privacy. *Automata, Languages and Programming. ICALP 2006. 4052*. Lecture Notes in Computer Science, Springer.

EDPB. (2025). *Guidelines 1/2025 on Pseudonymisation (version under public consultation)*. Retrieved from https://www.edpb.europa.eu/public-consultations/guidelines-012025-on-pseudonymisation_en

EDPS, & AEPD. (2025). *Techdispatch: Federated Learning*. Retrieved from https://www.edps.europa.eu/system/files/2025-06/techdispatch_federated-learning_en.pdf

ENISA. (2019). *Pseudonymisation techniques and best practices*. Retrieved from https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices

ENISA. (2021). *Post-Quantum Cryptography: Current state and quantum mitigation*. Retrieved from https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation

ENISA. (2024). *Engineering Personal Data Sharing*. Retrieved from https://www.enisa.europa.eu/publications/engineering-personal-data-sharing

ENISA. (2026). *ENISA's view on Cybersecurity in the Frontier AI Era*. Retrieved from https://www.enisa.europa.eu/publications/enisas-view-on-cybersecurity-in-the-frontier-ai-era

IDGDPT Berlin Group. (2024). *Working Papes on Data Sharing*. Retrieved from https://www.bfdi.bund.de/SharedDocs/Downloads/EN/Berlin-Group/20241206-WP-Data-Sharing.pdf?__blob=publicationFile&v=2

Lehmann, A. (2019). ScrambleDB: Oblivious (Chameleon) Pseudonymization-as-a-Service. *Proceedings on Privacy Enhancing Technologies*, (pp. 289-309).

Li, M., Yang, Y., Chen, G., Yan, M., & Zhang, Y. (2025). SoK: Understanding design choices and pitfalls of Trusted Executed Environments. *19th ACM Asia Conference on Computer and Communications Security (ASIA CCS '24)* (pp. 1600-1616). ACM.

NIST. (2020). *Security and Privacy Controls for Information Systems and Organizations, NIST SP 800-53 Rev. 5*. Retrieved from https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

NIST. (2020). *Zero-trust architecture*. NIST SP 800-207. Retrieved from https://csrc.nist.gov/pubs/sp/800/207/final

Ricciato, F. (2026). Privacy-enhancing or privacy-elusion technology? A critical view of (pseudo) synthetic data based on deep learning. *Journal of Official Statistics*. Retrieved from https://journals.sagepub.com/doi/10.1177/0282423X251412328

Ritchie, F. (2017). The 'Five Safes': A framework for planning, designing and evaluating data access solutions. *Data for Policy 2017:*. Retrieved from https://doi.org/10.5281/zenodo.897821

Robertson T., W. E. (2016). The importance of age, sex and place in understanding socioeconomic inequalities in allostatic load: Evidence from the Scottish Health Survey (2008-2011). *BMC Public Health*, p. 16:126.

Samarati, P. (2001). Protecting Respondents Identities in Microdata Release. (IEEE, Ed.) *IEEE Transactions on Knowledge and Data Engineering, 13*, pp. 1010-1027.

Sehgal, N. K., Bhatt, P. C., & Acken, J. M. (2020). Future trends in cloud computing. (S. International, Ed.) *Cloud Computing with Security*, pp. 235-259.

Sweeney, L. (2002). k-anonymity: a model for protecting privacy. *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10(7)*, pp. 557-570.

van Gastel, B., Jacobs, B., & Popma, J. (2021). Data Protection Using Polymorphic Pseudonymisation in a Large-Scale Parkinson's Disease Study. *J. Parkinsons Dis.*(11(s1)), pp. S19-S25.

Verheul, E., Jacobs, B., Meijer, C., Hildebrandt, M., & Ruiter, J. d. (2016). *Eric Verheul, Bart Jacobs, Carlo Meijer, Mireille HildPolymorphic Encryption and Pseudonymisation for Personalised Healthcare*. Eric Verheul, Bart Jacobs, Carlo Meijer, Mireille Hildebrandt and Joeri de Ruiter (2016), Polymorphic Encryption andCryptology {ePrint} Archive, Paper 2016/411. Retrieved from https://eprint.iacr.org/20

Zhou, I., Tofigh, F., Piccardi, M., Abolhasan, M., Franklin, D., & Lipman, J. (2024). Secure Multi-Party Computation for Machine Learning: A Survey. *IEEE Access*, pp. 53881–53899.


aepd
agencia
española
protección
datos


HELLENIC DATA
PROTECTION AUTHORITY