slices DS

HORIZON 2020
H2020 - INFRADEV-2019-3

D1.3 Analysis of legal compliance and regulation issues in Europe

Acronym	SLICES-DS
Project Title	Scientific Large-scale Infrastructure for Computing/Communication Experimental Studies – Design Study
Grant Agreement	951850
Project Duration	24 Months (01/09/2020 – 31/08/2022)
Due Date	31 August 2022 (M24)
Submission Date	19 September 2022
Authors	Sébastien Ziegler (MI), Adrian Quesada Rodriguez (MI), Cédric Crettaz (MI), Vasiliki Tsiompanidou (MI), Renáta Radócz (MI), Ekaterina Kasyanova-Kühl (MI)
Reviewers	All partners

Scientific Large-scale Infrastructure for Computing Communication Experimental Studies **Design Study**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 951850. The information, documentation and figures available in this deliverable, is written by the SLICES-DS project consortium and does not necessarily reflect the views of the European Commission. The European Commission is not responsible for any use that may be made of the information contained herein.

Executive Summary

SLICES Research Infrastructures intend to become a flexible platform aiming to support large-scale experimental research focuses on emerging technologies, including networking protocols, radio technologies, cloud and edge-based computing, etc. As such, it needs to consider a multitude of legal implications and regulations to successfully ensure compliance.

This Deliverable D1.3. lays down the foundation for SLICES' compliance with legal requirements, as evaluated during the design phase. Taking into consideration its innovative approach and the incorporation of emerging technologies from the onset of the project, the legal requirements presented cover a variety of sectors, that can be categorised as follows:

1. Scientific research and experimentation,
2. Data protection and privacy, and
3. Open Science.

After thoroughly defining the scope of the above, the present deliverable analyses existing and anticipated legislative instruments on a European level, distinguishing the provisions that are principally relevant to the SLICES project. The hereby included regulations, as well as any future amendments or updates, are to be considered throughout the SLICES' lifecycle to ensure compliance with legal requirements and ethical standards.

In addition to the above, the deliverable moves to the identification of potential legal risks that could endanger the project's smooth operation and evolution, followed by suggested mitigation measures. It also introduces a set of questions that need to be answered in order to establish and implement adequate administrative procedures, compliance and data protection policies, as well as to finalise the relevant organisational structure along with the precise and predetermined rights and obligations of each party.

Table of contents

1. Introduction

The deliverable D1.3 is reporting the results of the Task 1.3 and analyses different regulatory frameworks and legislation in order to identify and address the administrative procedures and legal compliance activities. This deliverable is also proposing some mitigations and contingencies to prevent any risks or threats for the future RI. Technical and operational requirements may be derived to minimise risks to the implementation phase of the Research Infrastructure. Furthermore, EOSC and FAIR principles are taken into account for the management of the open data.

2. Methodological Approach

This deliverable builds on and collects previously examined matters around the legal and ethical requirements for the SLICES project. In particular, this deliverable explores more in detail the requirements and considerations for the SLICES project for ethical research and experimentation activities, exploring dual-use and national restrictions on scientific activity. Then, data protection and data management legislative instruments on a European Union level are reviewed ranging from the well-known General Data Protection Regulation (GDPR) to upcoming legislation such as the Artificial Intelligence (AI) Act. Moreover, the requirements for open science are further explained. Finally, an overview of potential and existing legal risks identified is carried out, followed by a number of recommendations and guidelines for the uninterrupted and safe continuation of the project.

3. Scope Definition

3.1. Scientific Research and Experimentation Regulations

Ever since the establishment of the European Single Market, it became apparent that **innovation, supported by scientific research and experimentation**, was the **driving force to achieve the Union's constantly evolving goals**, to expand cooperation and extend its presence as a critical factor in the shaping of the global society[1]. Nonetheless, taking into consideration the multitude of countries forming the Union and the various differences in practice, the Union's policy was characterised by **fragmentation**, which, in turn, inhibited the rapid acceleration of science, research, and innovation[2].

For this reason, it was deemed essential to form a **series of rules and guidelines** that would promote scientific progress and research, **without compromising the Union's values and human rights**, particularly fostered through the Horizon2020 program that was launched in 2014[3], and has now been replaced by the Horizon Europe programme.

[1] European Commission. Directorate General for Research and Innovation., *Science, Research and Innovation Performance of the EU, 2020 :A Fair, Green and Digital Europe.* (LU: Publications Office, 2020), https://data.europa.eu/doi/10.2777/890488, [Last accessed 31 August 2022]

[2] McKinsey Global Institute, "Innovation in Europe - Changing the Game to Regain a Competitive Edge," October 2019, https://www.mckinsey.com/~/media/mckinsey/featured%20insights/innovation/reviving%20innovation%20in%20europe/mgi-innovation-in-europe-discussion-paper-oct2019-vf.ashx, [Last accessed 31 August 2022]

[3] European Commission. Directorate General for Research and Innovation. and PPMI., *Assessment of the Union Added Value and the Economic Impact of the EU Framework Programmes: Final Report.* (LU: Publications Office, 2017), https://data.europa.eu/doi/10.2777/065997, [Last accessed 31 August 2022]

In the present deliverable, the **requirements of the Horizon program** shall be examined, as well as the additional **conditions that must be met by researchers and scientists** in order to ensure that their work is **ethical and compliant with their legal obligations**. The **possible restrictions** on the scope of their research shall also be reviewed.

3.2. Data Protection and Management

Data has been occupying a more and more prominent position in the development of technology, fostering innovation and, therefore, digital societies. As a result, **data protection and management have been placed at the centre of the EU's innovation and digital strategy**, recognising the omnipresence of data in modern technological advancements, including not only personal data leading to identifiable natural persons, but also research and other related data[4].

Taking into consideration the above-described importance that the Union has attached to data, this deliverable will focus on **existing and future legislative initiatives** on a European level regarding data protection, data management, use and accessibility in different contexts, as well as data sharing. At the same time, **national provisions on research data requirements** shall be examined and reviewed.

3.3. Open Science

As previously explained, science and research form integral parts of innovation, economic and societal progress. In order, though, to fully exploit the advantages presented by scientific research, it is essential that the others have access to the methodology, tools, and results produced, in order to be able not only to implement, but also to further evolve it. Open Science describes precisely this movement of removing barriers in research and promoting open access to data, publications, software etc.

As such, it constitutes a central element in the Horizon Europe program, noting in particular that during the Horizon2020 program 83% of publications resulting from projects funded by the Union offered open access[5].

Of course, open access does not mean that copyright and intellectual property rights are obsolete and cannot be protected. On the contrary, it is important to balance them and estimate when open access should be preferred over copyright protection and vice versa.

The relevant section of this deliverable shall present the open science requirements on a private and public sector level, as well as the provisions for the protection of researchers' copyright.

[4] European Commission, "A Europe Fit for the Digital Age," 2019, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en, [Last accessed 31 August 2022]

[5] European Commission. Directorate General for Research and Innovation. et al., *Monitoring the Open Access Policy of Horizon 2020: Final Report.* (LU: Publications Office, 2021), https://data.europa.eu/doi/10.2777/268348, [Last accessed 31 August 2022]

4. Applicable Regulations for Scientific Research and Experimentation

4.1. Ethical Requirements

Researchers operating within the framework of the European Union (EU) are meant to abide by the **foundational rules and values** upon which the Union was built. As such, researchers who intend to introduce or have already introduced projects in the EU must follow certain **ethical requirements**. Even though ethics may originally be perceived as a rather abstract concept, the Union has managed to lay out a set of **concrete provisions**[6], which can be divided as follows:

1. **Data Protection and Privacy** requirements,
2. Research on **humans**, human cells or tissues, and human embryos requirements,
3. **Environment, health, and safety** requirements,
4. **Animal research** requirements,
5. **Artificial Intelligence** requirements, and
6. Research involving **non-EU countries'** requirements.

Taking the above into consideration, in continuation, the **relevant ethical requirements for SLICES** shall be presented. Starting with **data protection and privacy requirements**, they mainly reflect the principles included in the **Charter of Fundamental Rights of the European Union**[7] and the **Treaty on the Functioning of the European Union**[8]. The **principal issues** that need to be tackled by researchers refer to **using and sharing the data and guaranteeing privacy of natural persons and identifiable personal data**, where applicable, either by **pseudonymising or anonymising** their data where possible.

At the same time, personal data must be processed in accordance with certain principles and conditions that aim to limit the negative impact on the persons concerned and ensure **fairness, transparency and accountability** of the data processing, **data quality and confidentiality**, while it is always highlighted that all participants in the research must provide their **informed consent** unless the conditions for an exception are met[9].

Where **human participants** are involved, researchers must ensure that their research activities **respect** the persons involved as well as **human dignity,** while any selection and participation criteria must be **fair and non-discriminatory**. Of course, the **rights and interests of the participants** must always hold a prominent position in the research plan, highlighting once more the importance of informed consent. Where possible, it is advised to **avoid involving subjects of potentially vulnerable groups or sensitive personal data**, unless additional safeguards are priorly set in place.

Similarly, where **non-EU countries** are involved, a **risk assessment** must be conducted to verify that no danger is posed to participants, personal data, or the outcome of the research. Moreover, **additional**

[6] European Commission and Directorate General for Research, *Ethics for Researchers: Facilitating Research Excellence in FP7.* (Luxembourg: Publications Office, 2013), http://bookshop.europa.eu/uri?target=EUB:NOTICE:KI3213114:EN:HTML, [Last accessed 31 August 2022]

[7] European Council, "Charter of Fundamental Rights of the European Union (2000/C364/01)" (2000), http://www.europarl.europa.eu/charter/pdf/text_en.pdf, [Last accessed 31 August 2022]

[8] European Union, "Consolidated Versions of the Treaty on European Union and the Treaty on the Functioning of the European Union," October 26, 2012, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012M/TXT&from=en, [Last accessed 31 August 2022]

[9] European Commission and Directorate General for Research, *European Textbook on Ethics in Research* (Luxembourg: Publications Office, 2010), [Last accessed 31 August 2022]

safeguards must be implemented where that is required to protect the research project, while a **quality assessment of data and resources imported** from a non-EU country must be carried out.

Last but not least, when **Artificial Intelligence (AI) systems** shall be deployed, it is essential that researchers meet certain prerequisites[10]:

i. Natural persons must be able to **oversee AI and intervene,** when necessary,
ii. AI systems must be **technically robust and safe**,
iii. AI must **guarantee privacy and data protection** throughout its lifecycle, according to the principle of privacy by design and by default, while ensuring the quality, integrity and security of data,
iv. The decision-making process must be **transparent, well-documented, and communicated**,
v. AI systems must be **fair, unbiased and non-discriminatory**,
vi. AI systems must take into consideration and **avoid any harm to the society or the environment,**
vii. AI developers must assume **accountability** for their actions and any potential consequences,
viii. The **involvement of an ethics advisor or advisory board** is recommended to maintain a satisfactory level of protection.

All carried out research projects and/or experiments must abide by the principles of **sustainable development,** causing no harm to the environment and ensuring protection of future generations.

SLICES will also **abide by the All-European Academies (ALLEA) European Code of Conduct for Research Integrity**[11] principles of reliability, honesty, respect and accountability. Specifically, the Code of Conduct emphasises that its purpose is to help realise the basic responsibility of the research community, which is to formulate the principles of research, define the criteria for proper research behaviour, maximise the quality and robustness of research, and respond adequately to threats to or violations of research integrity. In doing so, the Code of Conduct recognises that Interpretation of the values and principles that regulate research may be affected by social, political or technological developments and by changes in the research environment. Surely, all research activities must promote the principles of **research integrity**, which can be defined to include **honesty in communication**, **reliability in performing research**, **objectivity**, **impartiality** and **independence**, **openness and accessibility, duty of care, fairness** in providing references and giving credit, and **responsibility** for the scientists and researchers of the future.

Careful attention will be given to ensuring that SLICES processes respect the aforementioned principles, in alignment with applicable law. The processes, methods and techniques for data collection and data management will respect the project's requirements, while also applying the utmost consideration for research subjects, study participants and all stakeholders involved. The project partners will take all measures necessary to refrain from practising any form of plagiarism, data falsification or fabrication. As far as data collection from human participants is concerned, SLICES will

[10] European AI Alliance, European Commission, "ALTAI - The Assessment List on Trustworthy Artificial Intelligence," n.d., https://futurium.ec.europa.eu/en/european-ai-alliance/pages/altai-assessment-list-trustworthy-artificial-intelligence#:~:text=The%20Assessment%20List%20for%20Trustworthy%20Artificial%20Intelligence%20%28ALTAI%29%2C, the%20trustworthiness%20of%20their%20AI%20systems%20under%20development, [Last accessed 31 August 2022]

[11] The European Code of Conduct for Research Integrity, (2017), https://www.allea.org/wp-content/uploads/2017/05/ALLEA-European-Code-of-Conduct-for-Research-Integrity-2017.pdf, [Last accessed 31 August 2022]

always inform participants about what data will be used, who will have access to the data, in what format the data will be accessed, which data protection rights apply to the data, and how long the data will be kept for. Any such activity will be coupled with the collection of voluntary informed consents from all participants, including consent for long-term storage of data or archiving. Privacy will be respected in this process and all personal data will be protected according to GDPR, national regulations, institutional regulations and data management standards.

In addition, the European Charter for Researchers provides a set of general principles and requirements and specifies the roles, responsibilities, and entitlements of researchers aiming at ensuring the balance between effective and ethical research[12]. According to it, researchers shall be bound by the following principles:

- Intellectual freedom;
- Adherence to recognised ethical practices and standards;
- Professional responsibility, avoiding plagiarism and duplicating work, maintaining a professional attitude;
- Fulfilment of contractual and legal obligations;
- Accountability, adhering to the principles of sound, transparent and efficient financial management;
- Good practice in research, taking all necessary precautions;
- Dissemination and exploitation of results, making them accessible to benefit society;
- Public engagement, ensuring non-specialists can access and comprehend their work;
- Fruitful supervision in a structured way;
- Responsibility of senior researchers to encourage and mentor future generations;
- Continual professional development.

Finally, consideration of ethical aspects must include the identification of ethical risks that may emerge from data collection and data management, including any data processing that needs to occur. These risks fall under different categories, according to the European Commission's Ethics and Data Protection report[13], a document that aims to raise awareness in the scientific community with regards to these issues. Risks related to different types of personal data may include data about racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic, biometric or health data, sex life or sexual orientation, and data about trade union membership. Risks with regards to specific data subjects may include data about children, vulnerable people or people who have not given their explicit consent to participate in a project. There are also risks regarding: (i) the scale or complexity of data processing, e.g., when we have large-scale processing of personal data; (ii) the data collection or processing technique used, e.g., when privacy-invasive methods are used or when artificial intelligence is used to analyse personal data; (iii) the involvement on non-EU countries, e.g., when collection of personal data is done outside of the EU or when there is transfer of personal data to non-EU countries.

SLICES will consider all indicators of data collection and management (including data processing) operations that may entail higher ethics risks. When such high risks are identified, a detailed analysis of any issues raised will take place, which must cover the following aspects, in alignment with EU's Ethics and Data Protection report: (i) an overview of all planned data collection and processing

[12] Euraxess, "The European Charter for Researchers" (2005), https://en.uoc.gr/files/items/7/7668/charter_code_for_researchers_en.pdf, [Last accessed 31 August 2022]

[13] Ethics and data protection, European Commission, https://ec.europa.eu/info/sites/info/files/5._h2020_ethics_and_data_protection_0.pdf, [Last accessed 31 August 2022]

operations; (ii) identification and analysis of the ethics issues that these raise; and (iii) an explanation of how these issues will be mitigated in practice. The analysis will be included in the research protocol and any relevant documentation for ethics approvals. Following ethics approval, records documenting informed consent procedures must be kept, so that these are available if requested by data subjects, funding agencies or data protection supervisory authorities.

4.2. Dual Use Restriction

Nonetheless, research activities and experimentation cannot be freely conducted in all sectors and fields. It has been long recognised that nearly every scientific or technological advancement can be used for **multiple purposes**, including for purposes **other than the ones originally envisioned**, often **leading even to their use for military and adverse purposes**[14]. For this reason, the Union has deemed it essential to provide an **adequate framework** that would ensure that **such misuse of technology is avoided.**

On one hand, dual use restrictions are placed due to the latest **Dual-Use Regulation**[15], regulating exports, brokering, technical assistance, transit, and transfer of dual-use items. In this context, dual-use items mean "***items, including software and technology***, *which can be* ***used for both civil and military purposes***, *and includes items which can be used for the design, development, production or use of* ***nuclear, chemical or biological weapons or their means of delivery***, *including all items which can be used for both non-explosive uses and assisting in any way in the manufacture of nuclear weapons or other nuclear explosive devices*"[16].

The Regulation explicitly recognises that among the persons that may be involved in the export of dual-use items there are researchers who often work on state-of-the-art technologies and, thus, require **further guidance to combat such risks** of using the outcome of their work for mischievous purposes[17]. **Restricted dual-use items are restricted as follows**:

- **Category 0:** Nuclear materials, facilities and equipment;
- **Category 1:** Special materials and related equipment;
- **Category 2:** Materials processing;
- **Category 3: Electronics;**
- **Category 4: Computers;**
- **Category 5:** Telecommunications and "information security";
- **Category 6:** Sensors and lasers;
- **Category 7:** Navigation and avionics;
- **Category 8**: Marine;
- **Category 9**: Aerospace and propulsion.

[14] European Commission, "EU Compliance Guidance for Research Involving Dual-Use Items," May 8, 2019, https://trade.ec.europa.eu/consultations/documents/consul_183.pdf, [Last accessed 31 August 2022]

[15] European Council, "Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 Setting up a Union Regime for the Control of Exports, Brokering, Technical Assistance, Transit and Transfer of Dual-Use Items" (2021), https://eur-lex.europa.eu/eli/reg/2021/821/oj, [Last accessed 31 August 2022]

[16] Article 2 par. 1 of the Dual-Use Regulation.

[17] Recital 13 of the Dual-Use Regulation.

Similarly, the above categories of restricted items are divided in the following **subcategories**:

- **A = Systems, equipment and parts**
- **B = Test, inspection and production equipment**
- **C = Materials**
- **D = Software**
- **E = Technology**

Specifically for the **software** subcategory, there are two main **exceptions to the controls** otherwise required, namely the case of **software that is generally available** to the public and software that is **already in the public domain**. Additionally, for the dual-use **technology** subcategory, there are three control **exceptions**, namely technology that is the **result of basic scientific research**, technology already **in the public domain** and technology that contains the **minimum required information for patent applications.**

Nonetheless, it is frequently noted that the majority of research activities do not occupy dual-use items within the limited scope of the Dual Use Regulation and are, therefore, not subject to the **export scrutiny** envisioned[18]. In this case, researchers are still invited to implement **self-control measures** to ensure that their projects are used in the proper manner, mainly reviewing their projects' potential reasonable uses, the safeguards in place and the acquisition of necessary authorisations for data circulations[19].

4.3. National Security Restrictions

In spite of the Union's support on the development of emerging technologies and the progress of scientific research, it would not be possible to omit Member States' national interests as a means of limitations on research and experimentation itself, as well as on its results.

In fact, **national security restrictions** are present throughout the Union's history and are even enshrined in the **Treaty on the Functioning of the European Union (TFEU)[20], providing derogations from a number of core EU freedoms**, such as:

- **Freedom of movement of imports, exports, and goods in transit[21],**
- **Freedom of movement for workers[22],**
- **Freedom of establishment[23], and**
- **Freedom of services[24].**

[18] Ibid rec. 6, p. 7.

[19] European Commission, "Data Protection and Privacy Ethical Guidelines," September 18, 2009.

[20] European Union, "Consolidated Versions of the Treaty on European Union and the Treaty on the Functioning of the European Union."

[21] Article 36 of the TFEU.

[22] Article 45 of the TFEU.

[23] Article 51 & 52 of the TFEU.

[24] Article 56 of the TFEU.

Such limitations placed in the case of research projects and experiments, in particular, could take the **following forms**[25]:

a. **Full prohibition or setting quotas** on technologies sensitive to national security,
b. **Prohibitions and restrictions on financing** foreign research in the fields sensitive to national interests,
c. **Prohibitions and restrictions for scientists on participation** in such research or publication of results in question.

It is, thus, understandable that the **Member States** can choose to restrict scientific research and experimentation in a number of ways if they judge that there are risks to their national security. Of course, even though the Union provides a basic set of guidelines, Member States can determine whether research or experiment poses a threat to their national security **at their own discretion**, based on their own **national legislation**. Any remedies toward such decisions are provided for by each Member State's national rules and laws.

5. Applicable Regulations for Data Protection and Management

5.1. GDPR

The **General Data Protection Regulation**[26] **(hereafter the GDPR)** has become the **main EU legislative instrument** in the sector of protection of personal data and the right to privacy since its application on May 25th, 2018. As an **intrinsic part of the European Single Market Strategy**, it mainly focuses on establishing a legal framework capable of maximising data protection by providing an enhanced set of rules for the Union, ensuring homogeneity among Member States, promoting innovation and adapting to the digital era.[27] The GDPR builds on the already existing, as a result of the Data Protection Directive, principles and obligations on data controllers and data processors, significantly expanding them.

In particular, the GDPR sets down the **principles for data collection and processing**[28] as follows:

a. Lawfulness,
b. Fairness,
c. Purpose, storage and time limitation,
d. Data minimisation,
e. Data protection by default and by design,
f. Accuracy, integrity and confidentiality of data, and
g. Transparency and accountability.

[25] Vitaliy Slepak, "National Security Clause: Law and Practice of European Union and Eurasia Economic Union," *Journal of Physics: Conference Series* 1406, no. 1 (November 1, 2019): 012002, https://doi.org/10.1088/1742-6596/1406/1/012002, [Last accessed 31 August 2022]

[26] European Council European Parliament, "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)," Pub. L. No. 32016R0679, 119 OJ L (2016), http://data.europa.eu/eli/reg/2016/679/oj/eng, [Last accessed 31 August 2022]

[27] "A Digital Single Market for the Benefit of All Europeans | Shaping Europe's Digital Future," accessed September 28, 2021, https://digital-strategy.ec.europa.eu/en/library/digital-single-market-benefit-all-europeans, [Last accessed 31 August 2022]

[28] Article 5 GDPR.

As the GDPR contains a number of provisions, the following points summarise the **most relevant GDPR provisions for SLICES stakeholders**:

- Personal data, in the context of the GDPR, refers to "*any information relating to an **identified or identifiable natural person***", in the sense of any person that can be identified with a reference to their name, identification number, location data, online identifiers, such as IP address, or their physical, physiological, genetic, mental, economic, cultural or social characteristics of said person.[29] In other words, the GDPR provides for a broad definition and, thus, **broad protection spectrum, of personal data,** including any information that can connect the data collected to a specific person.
- The GDPR applies to the **processing of personal data of natural persons by legal entities based or having branches within the EU territory**,[30] as well as by legal entities that, in spite of being based outside the Union, **offer goods or services, physical or digital, within the EU**, regardless of the final location of storage and/or processing.[31] This means that, as long as services are being provided in the EU, the GDPR shall apply regardless of whether the data will be ultimately stored or processed and regardless of the data subjects' nationality.
- In order for the GDPR to apply, **wholly or partly automated means** must have been employed for the processing, including if said means form or are intended to form part of a filing system.[32]
- **Data that has been anonymised**, i.e., that can no longer lead to an identifiable individual, does not fall within the scope of the GDPR, as per Recital 26 of the GDPR.
- In order for the processing of personal data to be considered lawful, it should be conducted **on one of the following legal bases** as required by Art. 6 (1) of the GDPR:
  i. **Consent of the data subject:** Consent can be used as an appropriate lawful basis under the condition that data subjects are offered a genuine choice when choosing whether they shall allow or forbid the collection, storage and processing of their data. What is more, it must meet the following additional conditions[33]:
     - **Consent must be freely given:** Consent must exclude any elements of inappropriate pressure and influence, deception, intimidation or coercion which would prevent the data subject from expressing and exercising their free will without detriment.[34] It goes without saying that where there is an imbalance of powers, for instance in hierarchical employment relationships, or where consent is tied to the performance of a contract and is included in a non-negotiable part of terms and conditions, it is considered to not be freely given. The EDPB guidelines also highlight the need for granularity in consent, in the sense that data subjects must be able to choose the exact purposes for which they allow their data to be processed.
     - **It must be specific:** Consent must be given for "one or more specific" purposes, without allowing for a gradual widening or blurring of said purposes (the so-called "function creep"). As mentioned above, data subjects should be provided separate opt-ins for each purpose, securing granularity. Additionally, and in spite of the principle of purpose

[29] Article 4 GDPR.

[30] Articles 1-2 GDPR.

[31] Article 3 GDPR.

[32] Article 2 GDPR.

[33] Article 7 GDPR.

[34] EDPB Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1, Adopted on 4 May 2020; accessible here: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf, [Last accessed 31 August 2022]

limitation[35], data subjects may give their consent for multiple processing activities carried out for the same purpose.[36]

- **It must be informed:** In accordance with the principle of transparency, data subjects must be provided with all information regarding the controller's identity, the purpose of each processing operation, the type of data that shall be collected and the consequences of their choice in a plain and easily understandable language. In addition, they need to be informed about the right to withdraw consent and how to do that, as well as for any automated decision-making taking place.
- **It must be seen as an unambiguous indication of the data subjects' wishes:** Consent needs to be the result of clear affirmative action, i.e., through an active motion or declaration, including electronic statements. Of course, preselected options, such as pre-ticked opt-in or opt-out constructions, silence or inactivity do not meet the said requirement.

ii. **Necessary for the performance of a contract with the data subject:** The processing is not required to be the sole way to perform the contract or the required pre-contractual steps, but it can be a proportionate integral part to perform the contract with this particular person. It is, thus, subject to a strict interpretation of necessity and proportionality.

iii. **Compliance with legal obligations:** It is not important whether the legal obligation is prescribed by EU, international or national provisions, as long as the processing, collection and storage is required to comply with a requirement provided by a concrete piece of legislation.

iv. **Protection of vital interests of data subjects:** This lawful basis includes only the cases of processing where the life or health of a natural person is at stake and is meant to be viewed as an exceptional ground for processing.[37]

v. **Performance of a task carried out in the public Interest:** This includes either a task in the public interest prescribed by law or undertaking official authority as required by law. The specific task shall be traced back to a concrete piece of legislation, clearly identifying the function or power granted to the controller/processor.

vi. **Legitimate Interest:** Even though it is a rather flexible lawful basis, it must be linked to a specific legitimate interest of the data subjects and is subject to a three-fold test of purpose, necessity and balance.

- **Special categories of data**: Where the processing involves personal data classified as special categories they require special treatment and need to have a separate lawful basis, as per Articles 8-10 of the GDPR. Such data, however, shall not be collected and/or processed within the SLICES project.
- **Further processing**: In order to utilise the data for purposes other than those originally collected shall be based in one of the lawful bases of Article 6 of the GDPR, unless said additional purpose is compatible with the purpose for which the personal data is initially collected[38].
- **Rights of the data subjects**: SLICES is bound to respect the data subjects' rights, as described in Chapter III of the GDPR (Articles 12 - 22), as further explained in the project's Data Management Plan.
- In particular, as per Article 22 GDPR, the data subjects maintain the right to not be subject to **profiling and automated decision-making**, unless the following conditions are met:

i. The decision is necessary in order to enter into or perform a contract with the data controller; or

[35] Article 5(1)(b), GDPR.
[36] GDPR Recital 32.
[37] Recital 46 GDPR.
[38] Recital 50 GDPR.

ii. The automated processing is authorised by the Union's or Member-States' law and includes suitable measures to safeguard the data subject's rights, freedoms and legitimate interests; or
iii. The data subjects have provided their explicit consent.

- **Security of processing**: Each controller or processor of personal data must ensure that they have adopted appropriate technical and organisational measures to protect said data from any risks indicatively due to unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data[39].
- **Notification of personal data breaches**: A detailed data breach plan is included in Deliverable SLICES-DS D1.7.
- **Data Protection Officer (DPO):** Appointment of a DPO is required where: *(i) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; or (ii) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or (iii) the core activities of the controller or the processor consist of processing on a large scale of special categories*.[40]
- **Data Protection Impact Assessment (DPIA)**: Where processing is carried out, in particular, using new technologies and is likely to result in a high risk for the rights and freedoms of data subjects, it is necessary that an assessment of the processing's impact is conducted under the DPO's supervision[41].

5.2. EPrivacy

5.2.1. EPrivacy Directive

Directive 2002/58/EC, in short, the **ePrivacy Directive**,[42] has been in force in the Union since July 2002, as was amended in 2009. The Directive, also known as "**the cookie directive**", given that the regulation of cookies in websites is at the core of the legislation, precedes the GDPR and complements the framework on data protection and privacy in the sector of electronic communications. Taking into consideration that the legislative instrument chosen was the Directive, the Member-States were obliged to transpose it to their national legal order, thus leaving room for **divergences[43]**.

In particular, the Directive applies to the **processing of personal data in the context of available electronic communication services available at public networks**, as well as subscriber lines connected to digital and analogue, where possible, exchanges.[44] In the context of the ePrivacy Directive, subscribers may be **natural or legal persons or businesses** providing **services within EU territory**[45].

[39] Article 32 GDPR.

[40] Article 37 GDPR.

[41] Article 35 GDPR.

[42] European Parliament, "Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications)," December 6, 2002, available at: https://eur-lex.europa.eu/legal-content/EN/, , [Last accessed 31 August 2022]

[43] Timelex, SMART for the European Commission, "EPrivacy Directive: Assessment of Transposition, Effectiveness and Compatibility with Proposed Data Protection Regulation," 978-92-79-47439-2, 2015, https://digital-strategy.ec.europa.eu/en/library/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data, [Last accessed 31 August 2022]

[44] Article 3 of the ePrivacy Directive.

[45] Article 1 of the ePrivacy Directive.

Taking into consideration the **sensitive nature** of these services, service and network providers are obliged to adopt **appropriate technical and organisational security measures**, taking into consideration the **state of the art**, while they are also obliged to inform the data subjects of any breaches and their implications[46]. They must also ensure **confidentiality of communications and traffic data**, prohibiting any type of monitoring without the users' explicit consent following the provision of clear and comprehensive information[47].

In fact, **consent** is deemed crucial to prevent the intrusion of users' privacy and unsolicited tracking that can be carried out by hidden identifiers and similar devices that can gain, store or trace the users' information and activity[48]. **Cookies**, for instance, are recognised to be falling within the scope of such tracker devices as legitimate and useful tools for business purposes, as long as the relevant data protection conditions are met, namely the provision of clear and precise information, the definition of legitimate purposes, the users' consent and opt-out opportunities[49].

On that note, one of the most innovative provisions of the Directive, as prescribed by its Article 6, lies with the classification of **traffic data**, i.e., "*data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof*", **as personal data**. As such, they are subject to the **data protection principles** of data minimisation, anonymisation, limitations on the storage period, consent and its withdrawal, access and purpose limitations, as well as to the data subjects' right to information and transparency. The same applies to **location data** other than traffic data[50].

Where data is to be stored in **public directories**, users, whether natural or legal persons, need to be informed of said storage, the usage as well as the recipients of the data. Similarly, **transmissions** must be based on safety measures and be conducted in accordance with the purposes for which the data was initially collected or in accordance with the data subjects' updated consent[51].

In spite of the fact that the ePrivacy Directive has been deemed insufficient by the European Union, it has been confirmed that the purposes for which it was first adopted, as well as its goals, remain relevant in the shaping of the Union's future framework on this field. As such, providers of these services must ensure compliance with the obligations laid down in the Directive until its replacement/revision.

5.2.2. EPrivacy Regulation

As was noted above, the ePrivacy Directive has not fully achieved the goal of harmonising privacy and electronic communications legislation within the Union, with multiple voices raising the need for the Directive's replacement with a Regulation for a number of years[52]. As such, discussions on an **ePrivacy Regulation**[53] started in July 2017, looking to **expand the existing framework and bring it up to date**

[46] Article 4 of the ePrivacy Directive.

[47] Article 5 of the ePrivacy Directive.

[48] Recital 24 of the ePrivacy Directive.

[49] Recital 25 of the ePrivacy Directive.

[50] Article 9 of the ePrivacy Directive.

[51] Recitals 38-39 of the ePrivacy Directive.

[52] Timelex, SMART for the European Commission, "EPrivacy Directive: Assessment of Transposition, Effectiveness and Compatibility with Proposed Data Protection Regulation." , [Last accessed 31 August 2022]

[53] European Commission, "Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC

with the - already in force – GDPR. Of course, the Regulation is intended to still leave a margin of discretion preserved for Member States, should they desire to introduce further national provisions in accordance with the spirit of the Regulation[54].

The envisioned ePrivacy Regulation, which shall apply in public electronic communications services offered to the Union's end-users[55] and shall be overseen by the European Data Protection Board (hereafter EDPB)[56], focuses on **6 main pillars**[57], involving:

i. **More players** of electronic communications services,
ii. A set of **stronger yet simpler rules** on data protection,
iii. The **expansion of protected activities** to include additional content and metadata,
iv. **Protection against spam**,
v. More effective **enforcement**,
vi. **New business opportunities.**

It is intended to be divided, more specifically, into the **following sections**:

Chapter I	Subject matter, scope and definitions
Chapter II	Confidentiality of electronic communications and users' consent, permitted purposes and conditions of processing, protection requirements
Chapter III	Rights of users and security risks
Chapter IV	Supervision and enforcement of the Regulation
Chapter V	Remedies of users and penalties for breaches
Chapter VI	Delegated and Implementing Acts
Chapter VII	Final provisions

The draft Regulation starts with the acceptance that **the content of electronic communications can reveal highly sensitive information about the users, whether natural or legal persons,** that if they were to become public without their consent could have detrimental effects to their overall societal and economic position. Taking that into consideration, it also recognises that the **same risks apply to metadata that can lead to the creation of an extremely accurate picture regarding the persons and businesses involved** in electronic communications[58].

(Regulation on Privacy and Electronic Communications)" (2017), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010, [Last accessed 31 August 2022]

[54] Recital 7 of the draft ePrivacy Regulation.

[55] Recital 9 of the draft ePrivacy Regulation.

[56] Article 19 of the draft ePrivacy Regulation.

[57] European Commission, "Shaping Europe's Digital Future: Proposal for an EPrivacy Regulation," February 2022, https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation, , [Last accessed 31 August 2022]

[58] Recitals 2-3 of the draft ePrivacy Regulation.

For the above reasons, Article 6 of the draft Regulation provides a list of **conditions for providers electronic communications networks and services to fulfil in order to process electronic communications**, namely:

a. The processing must be **necessary to achieve the transmission** of the communication, as long as the criteria of necessity and proportionality as to the retainment period are met, or
b. The processing must be **necessary to maintain or restore the security** of the network or service or to fix technical errors.

In particular as to the providers of electronic communications services, they must additionally meet the **following requirements**:

A) When processing metadata:

1) The processing must be **necessary to meet mandatory quality of services**, or
2) The processing must be **necessary for billing and interconnection payments, for detecting or ceasing fraudulent or abusive actions**, or
3) The processing must be **based on the users' consent** for the already specified purposes, and

B) When processing the content of electronic communications:

1) Processing must be conducted for **the sole purpose of providing specific services** to end-users, as long as they have provided **consent**, recognising that said processing is indispensable, or
2) Processing must be **necessary for the specified purposes** for which the users have provided **consent** and the **Supervisory Authority has authorised** it.

Furthermore, as with all recent data protection legal instruments, the Regulation shall provide for the **erasure of the communications content and metadata or their anonymisation** once the purposes have been achieved/concluded[59]. Similarly, Article 8 sets out a strict framework of conditions under which the processing and storage of information from end-users' equipment is allowed.

The draft Regulation dedicates its entire Chapter III to the **rights of end-users** to control the sending and reception of electronic communications to protect their privacy, guaranteeing anonymity[60] and its limitations[61], while providing the conditions under which end-users may be included in publicly available directories[62]. Providers of electronic communications services are, based on this Chapter, required to alert end-users in case of risks to the security of networks and services, complementing the requirements with the ones laid down in the GDPR[63]. As far as **remedies, the right to compensation and liability are concerned**, the draft Regulation refers back to the GDPR[64].

[59] Article 7 of the draft ePrivacy Regulation.
[60] Article 12 of the draft ePrivacy Regulation.
[61] Article 13 of the draft ePrivacy Regulation.
[62] Article 15 of the draft ePrivacy Regulation.
[63] Article 17 of the draft ePrivacy Regulation.
[64] Articles 21-23 of the draft ePrivacy Regulation.

Even though the Regulation is not expected to enter into force before 2023, as negotiations are still ongoing[65], providers of electronic communications services, platforms and networks are advised to start preparations on abiding by the new provisions and requirements.

5.3. Data Act

As part of the wider European Strategy for data, through which the European Union is aiming at occupying a leading position in modern societies driven by data, the Data Act[66] was put forward in February 2022, principally aiming at **enhancing data use and accessibility** to reenforce the Union's market[67].

The proposed legal text, which has adopted the form of a **Regulation** to ensure uniformity, focuses on the following **main steps**[68] to achieve its goals, namely:

a. Enabling users of connected devices **to gain access to data generated by them and share them** as desired, without this meaning that manufacturers will be bearing additional costs or that the data generated by them will be used in direct competition with them,
b. **Rebalancing the negotiation power** of Small and Medium-sized Enterprises (SMEs) during their contractual relationships with stronger players,
c. Enabling users to **switch between different cloud data-processing service providers** while **preventing unlawful data transfers**.
d. Reviewing the Database Directive's provisions on **data derived by Internet-of-Things (IoT) devices to facilitate their use**.

The proposed Regulation is meant to be read and applied **in conjunction with the Data Governance Act**, as the two main legal instruments of the strategy for data.

In particular, the Regulation is meant to apply to the **following players**, as per Article 1 par. 2 of the Draft Data Act:

(a) ***manufacturers*** *of products and suppliers of related services placed on the market in the Union and the* ***users*** *of such products or services;*
(b) ***data holders*** *that make data available to data recipients in the Union;*
(c) ***data recipients*** *in the Union to whom data are made available;*
(d) ***public sector bodies and Union institutions, agencies or bodies*** *that request data holders to make data available where there is an exceptional need to that data for the performance of a task carried out in the public interest and the data holders that provide those data in response to such request;*
(e) ***providers of data processing services*** *offering such services to customers in the Union*.

[65] Härting Rechtsanwälte, "EPrivacy Regulation: EU Council Agrees on the Draft," March 24, 2022, https://www.lexology.com/library/detail.aspx?g=2c0eca0b-c828-4fd6-ac0f-21fdbeded2bb, [Last accessed 31 August 2022]

[66] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on Harmonised Rules on Fair Access to and Use of Data (Data Act)" (2022), https://digital-strategy.ec.europa.eu/en/library/data-act-proposal-regulation-harmonised-rules-fair-access-and-use-data, [Last accessed 31 August 2022]

[67] European Commission and Directorate-General for Communication, *Data Act: The Path to the Digital Decade.*, 2022, https://op.europa.eu/publication/manifestation_identifier/PUB_NA0722080ENN, [Last accessed 31 August 2022]

[68] European Commission Press Corner, "Data Act: Commission Proposes Measures for a Fair and Innovative Data Economy," February 23, 2022, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113, [Last accessed 31 August 2022]

The draft Regulation additionally describes how data sharing between businesses and consumers and among businesses may be carried out. In that context, **the users must be provided in advance with a minimum of information on the data that the product or service will generate, collect and process, who will have access to it and how users can access it, share it and defend their rights**[69]. Third parties with whom the users choose to share their data must process it **in accordance with the users' true wishes and respect data protection principles**[70].

At the same time, data holders must **ensure that data can be made available to any data recipients** required by the users, by the Union, or national legislation **in a fair, reasonable and non-discriminatory manner**, providing for a **reasonable compensation** for doing so, where applicable[71]. This also applies in cases where data sharing with a public sector body or a Union institution, agency or body is required by law and the data holder does not fall under the category of a small or micro enterprise[72]. Certainly, **technical protection measures** must be in place to safeguard the data and their accuracy, while hindering any unauthorised use or access to it[73].

Furthermore, the Regulation is intended to impose a series of **requirements for operators of data spaces aiming at facilitating interoperability of data**. In particular, operators must ensure, as per Article 28, that:

i) *the dataset content, use restrictions, licences, data collection methodology, data quality and uncertainty shall be **sufficiently described to allow the recipient to find, access and use the data;***

ii) *the data structures, data formats, vocabularies, classification schemes, taxonomies and code lists shall be **described in a publicly available and consistent manner**;*

iii) *the **technical means to access the data**, such as application programming interfaces, and their terms of use and quality of service **shall be sufficiently described to enable automatic access and transmission of data between parties**, including continuously or in real-time in a machine-readable format;*

iv) *the means to enable the **interoperability of smart contracts** within their services and activities shall be provided.*

The Regulation also includes a set of requirements regarding **open interoperability of data services**, as well as **smart contracts for data sharing** where that is applicable[74]. Finally, it is clarified that the right prescribed in Article 7 of the Database Directive, i.e., "*the right for the maker of a database which shows that there has been **qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents to prevent extraction and/or re-utilisation** of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database*", **does not apply to databases containing data obtained from or generated by the use of a product or a related service**[75].

[69] Articles 3-5 of the draft Data Act.

[70] Article 6 of the draft Data Act.

[71] Articles 8-9 of the draft Data Act.

[72] Chapter V of the draft Data Act.

[73] Article 11 of the draft Data Act.

[74] Articles 29-30 of the draft Data Act.

[75] Article 35 of the draft Data Act.

5.4. Data Governance Act

The **Data Governance Act (DGA)**[76], introduced on 25 November 2020 and approved in May 2022, has become the **first legislative initiative** to be adopted within the context of the **European Strategy for Data** aiming at **facilitating data-sharing** and creating a **robust framework for use of data for research purposes.**

In particular, the DGA provides for the **re-use of data held by public sector bodies**, which are protected on the grounds of commercial and statistical confidentiality, protection of intellectual property rights or the protection of personal data, but not to data held by public undertakings or by public service broadcasters and their subsidiaries or by cultural establishments and educational establishments, data protected for reasons of national security, defence or public security or data the supply of which is an activity falling outside the scope of the public task of the public sector bodies concerned as defined by law or by other binding rules in the Member State concerned[77].

Such public sector bodies shall make public the **conditions for allowing the re-use** of the above data, which must be **non-discriminatory, proportionate and objectively justified** taking into consideration the purposes of re-use and the nature of data, **and may include:**

a. The re-use solely of data that has been **pseudonymised or anonymised**,
b. The access and re-use the data within a **secure processing environment** provided and controlled by the public sector,
c. The access and re-use the data within the **physical premises** in which the secure processing environment is located, if remote access cannot be allowed without jeopardising the rights and interests of third parties,
d. Conditions to preserve the **integrity of the technical systems** of the secure processing environment used.
e. Conditions to preserve the **confidentiality** of data,
f. Conditions to preserve the **intellectual property rights**
g. Conditions on the further **transfer of data**[78].

It is, thus, **prohibited to implement agreements or other practices granting exclusive rights or restricting the availability** of data for re-use by other parties, **unless that is necessary for the provision of a service or a product in the general interest, in compliance with applicable Union and national public procurement and concession award rules**, or, in the case of a contract of a value for which neither Union nor national public procurement and concession award rules are applicable, in compliance with the principles of transparency, equal treatment and non-discrimination on grounds of nationality[79].

The re-use of data **may be subject to fees,** as long as they are non-discriminatory, proportionate and objectively justified, without restricting competition[80].

[76] European Parliament and Council of the European Union, "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European Data Governance (Data Governance Act)," November 25, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767, [Last accessed 31 August 2022]

[77] Article 3 of the draft DGA.

[78] Article 5 of the draft DGA.

[79] Article 4 of the draft DGA.

[80] Article 6 of the draft DGA.

The Regulation additionally lays out the **requirements applicable to data sharing services**. In particular, it introduces a **notification procedure** for the following data sharing services:

1. **Intermediation services** between **data holders which are legal persons and potential data users,**
2. **Intermediation services between data subjects that seek to make their personal data available** and potential data users,
3. **Services of data cooperatives**[81].

Data sharing shall be subject to a number of **conditions** laid out in Article 11 of the draft Regulation and including that:

1) *"the provider **may not use the data for which it provides services for other purposes** than to put them at the disposal of data users and data sharing services shall be placed in a separate legal entity;*
2) *the **metadata** collected from the provision of the data sharing service may be used only for the development of that service;*
3) *the provider shall ensure that the **procedure for access to its service is fair, transparent and non-discriminatory** for both data holders and data users, including as regards prices;*
4) *the provider shall **facilitate the exchange of the data** in the format in which it receives it from the data holder and shall convert the data into specific formats only to enhance interoperability within and across sectors or if requested by the data user or where mandated by Union law or to ensure harmonisation with international or European data standards;*
5) *the provider shall have **procedures in place to prevent fraudulent or abusive practices** in relation to access to data from parties seeking access through their services;*
6) *the provider shall ensure a **reasonable continuity of provision of its services** and, in the case of services which ensure storage of data, shall have sufficient guarantees in place that allow data holders and data users to obtain access to their data in case of insolvency;*
7) *the provider shall put in place **adequate technical, legal and organisational measures in order to prevent transfer or access to non-personal data that is unlawful** under Union law;*
8) *the provider shall take measures to ensure a **high level of security for the storage and transmission** of non-personal data;*
9) *the provider shall have procedures in place to ensure **compliance with the Union and national rules on competition;***
10) *the provider offering services to data subjects shall act **in the data subjects' best interest** when facilitating the exercise of their rights, in particular by advising data subjects on potential data uses and standard terms and conditions attached to such uses;*
11) *where a provider provides tools for obtaining consent from data subjects or permissions to process data made available by legal persons, it shall specify the jurisdiction or jurisdictions in which the data use is intended to take place."*

The above-listed conditions **shall not apply to non-profit entities that solely focus on collecting data for reasons of general interest that are later made available on the basis of data altruism**[82]. Such data altruism organisations shall be registered in a specified record, after their request, as long as they meet the necessary requirements, i.e., they are legal entities serving objectives of general interest, they

[81] Article 9 of the draft DGA.

[82] Article 14 of the draft DGA.

operate independently on a non-profit basis and they possess a legally independent structure to perform the activities related to data altruism[83].

Any organisation recognised as a data altruism organisation is obliged to keep full and accurate records regarding the persons processing data, the date and duration of such processing, the purposes and fees paid, in addition to an annual activity report to be submitted to the authorities, while ensuring protection of data holders' rights[84].

5.5. Digital Services Act

Recognising the need to modernise the e-Commerce Directive, the EU introduced in December 2020 the Digital Services Act[85], which was finally agreed upon in April 2022. Thus, the Digital Services Act (DSA) focuses on the introduction of **new prerequisites for platforms offering intermediary digital services in the Union's market**[86].

More specifically, the draft Regulation sets out a set of rules on the **liability of providers of intermediary services** including the following provisions:

- **Mere conduit,** meaning the mere transmission in a communication network of information provided by a recipient of the service, renders the service provider not liable as long as they do not initiate the transmission, nor choose the received and the information contained[87],
- **Caching**, meaning the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission, render the service provider not liable if they do not modify the information, they comply with the conditions on access, update and lawful use of technology and they act expeditiously to remove or to disable access when required[88].
- **Hosting**, meaning the storage of information, renders the service provider not liable if they do not have actual knowledge of illegal activity or content and of the respective facts or circumstances of the illegal activity or content, and, once obtaining such knowledge, acts expeditiously to remove or disable access[89].

Of course, there is **no general obligation to monitor the information transmitted or stored through the intermediary service providers**, but they shall act upon orders issued by the competent authorities on illegal content and provide all information necessary[90].

In addition to the above, service providers are subject to a number of **due diligence obligations** for a transparent online environment, establishing a **single point of contact for direct communication**, including all information necessary in their terms and conditions and shall conduct transparency

[83] Articles 15-17 of the draft DGA.

[84] Articles 18-19 of the draft DGA.

[85] European Parliament and Council of the European Union, "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and Amending Directive 2000/31/EC," 2020, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN, [Last accessed 31 August 2022]

[86] Article 1 of the draft DSA.

[87] Article 3 of the draft DSA.

[88] Article 4 of the draft DSA.

[89] Article 5 of the draft DSA.

[90] Articles 7-9 of the draft DSA.

reports annually on any content moderation they engaged in[91]. Moreover, they shall establish **adequate procedures and mechanisms to allow for individuals or entities to notify them of any illegal content**, while providing a statement of reasons for any decision to remove content[92].

The Regulation also provides for additional provisions applicable to **large online platforms**[93], focusing on an **internal complaint-handling system** against decisions to remove or disable access to content, to suspend or terminate the provision of services and to suspend or terminate the recipients' account[94]. They shall additionally take appropriate **measures against misuse of their platforms**, while also ensuring that any traders operating through their platform shall be traceable[95].

Moreover, specifically in the case of **very large online platforms**, they are obliged to carry out a **risk assessment at least on an annual basis** of the services provided, in specific on whether illegal content has been disseminated, on any potential negative effects on human rights and any intentional manipulation of their services[96]. Where risks were identified, they shall implement adequate mitigation measures, which shall be later controlled through an independent audit[97].

The Commission is to **support the introduction of further protocols, guidelines and Codes of conduct** for online service providers aiming at a completer and more comprehensive protective framework.

5.6. Database Directive

Pursuant to the 1991 action plan "Follow-up to the Green Paper on Copyright and the Challenge of Technology" and in view of the potential of an information market for the expansion of the EU, it was deemed essential to harmonise the legislation within its Member-States regarding the protection of databases, introducing Directive 96/9/EC on the **legal protection of databases**[98], whether **physical or electronic[99].**

It can be claimed that the Directive establishes a **dual system of protection**, focusing on **copyright protection of the database itself**[100] and establishing a ***sui generis* intellectual property right on the content of the database**[101] respectively. More specifically, the Directive proceeds to the following distinction:

1. The **protection of the database**, and not its content, by copyright, as long as it is the author's own intellectual creation, either due to its selection or arrangement of content.
   - As the **author** is deemed any natural person or group of natural persons who created the base or, where the legislation of the Member States so permits, the legal person designated as the

[91] Articles 10-13 of the draft DSA.

[92] Articles 14-15 of the draft DSA.

[93] Article 16 of the draft DSA.

[94] Article 17 of the draft DSA.

[95] Articles 20, 22 of the draft DSA.

[96] Article 26 of the draft DSA.

[97] Articles 27-28 of the draft DSA.

[98] European Commission, "Directive 96/9/EC of the European Parliament and of the Council of the European Union of 11 March 1996 on the Legal Protection of Databases" (1996), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31996L0009, [Last accessed 31 August 2022]

[99] Article 1 of the Database Directive.

[100] Article 3 of the Database Directive.

[101] Article 7 of the Database Directive.

rightsholder. When it is the result of collective work, as per national legislation, the economic rights are owned by the respective copyright holder, while when it is the result of a joint effort, exclusive rights are owned jointly as well[102].

- The rightsholder has, thus, the **exclusive right to conduct and/or authorise**[103]:

i. *"The **temporary or permanent reproduction** by any means and in any form, in whole or in part;*
ii. *The **translation, adaptation, arrangement and any other alteration**;*
iii. ***Any form of distribution** to the public of the database or of copies thereof. The first sale in the Community of a copy of the database by the rightholder or with his consent shall exhaust the right to control resale of that copy within the Community;*
iv. ***Any communication, display or performance** to the public;*
v. ***Any reproduction, distribution, communication, display or performance** to the public of the results of the acts referred to in (b)".*

- The above exclusive right **may be bypassed if one of the following conditions** are met and as long as the **rightsholder's legitimate interests remain protected**[104]:
  a. The exercise of any of the actions is **required by the lawful users to access the content** of the database and use it,
  b. The national legislation provides for the **possibility to reproduce a non-electronic database for private purposes**,
  c. The national legislation provides for the **possibility to use the database for the purpose of illustration for teaching or for scientific research**, where no commercial purpose is to be achieved,
  d. The national legislation provides for the **possibility to use the database for public security purposes or to achieve an administrative or judicial goal**,
  e. The national legislation provides for **other exceptions.**

2. The **protection of the content of the database** where its creator has substantially invested, qualitatively and/or quantitatively, in either the obtaining, verifying or presenting of the contents to prevent extraction and/or re-utilisation, not including public lending in the definition. **Such right may be transferred, assigned, or granted** under a contractual licence.

- The creators of the database content, whether natural persons or legal entities, are granted protection as long as they are **nationals of a Member State or they have their habitual residence in the EU,** in the EU, or – in case of legal persons -they have been established in accordance with the law of a Member State or they have their registered office, central administration or principal place of business within the EU, unless specific agreements have been put in place with third-country persons or entities and the Council[105].
- **Lawful users** of the database may extract or re-utilise parts of the contents, as long as they do not harm the rightsholders legitimate interests[106].
- **National legislation may stipulate exceptions**[107] to the sui generis right, in the following cases:
  a. When the contents of a non-electronic database are **extracted for private purposes,**
  b. When the extraction is **carried out to illustrate for teaching or for scientific research,** where no commercial purpose is to be achieved,

[102] Article 4 of the Database Directive.
[103] Article 5 of the Database Directive.
[104] Article 6 of the Database Directive.
[105] Article 11 of the Database Directive.
[106] Article 8 of the Database Directive.
[107] Article 9 of the Database Directive.

c. When there are **reasons of public security or to achieve an administrative or judicial goal.**

- The *sui generis* right is protected for a **period of fifteen years** starting from the first of January of the year following the date of completion or from when the database was first made available to the public. Where **substantial changes** are made, the resulting databased benefits from its own term of protection[108].

The above rightsholders are entitled to **appropriate remedies** according to the national legal order to protect said rights against infringements[109]. As was explained, and following the findings on the impact of the Directive[110], **the above *sui generis* right does not apply in cases of public sector bodies** in accordance with the open science principles.

5.7. Network and Information Security Directive

5.7.1. NIS1 (current version)

As of 2016, the EU has introduced the **first EU-wide legislative instrument on cybersecurity Network and Information Security Directive (hereafter NIS1)**[111] as an inextricable part of its b. As the chosen legal instrument was a directive, Member States had until 2018 to transpose the provisions to their national legislation but were free to adopt a more protective framework[112].

he NIS1 Directive can be divided in three parts, namely:

1. **National cybersecurity capabilities**[113], providing the following:
   a. Member States shall adopt national cybersecurity strategies, clearly defining the objectives, priorities, measures, training, research, actors and a risk assessment.
   b. Member States shall designate competent authorities to monitor the application of the directive, as well as a single point of contact to ensure cross-border cooperation.
   c. Member States shall designate one or more computer security incident response teams (CSIRTs), allocating adequate resources and building robust infrastructure.
   d. All the above-mentioned authorities are expected to cooperate with each other.
2. **Cross-border collaboration**[114], including:
   a. The establishment of a Cooperation Group, composed by representatives of the Member States, the Commission, and ENISA, tasked with providing strategic guidance and facilitating knowledge information sharing among the Member States.
   b. The establishment of a CSIRT network mainly focused on exchanging information and forwarding cooperation.
   c. The potential of signing international cooperation agreements.

[108] Article 10 of the Database Directive.

[109] Article 13 of the Database Directive.

[110] European Commission, "Commission Staff Working Document: Evaluation of Directive 96/9/EC on the Legal Protection of Databases," April 25, 2018, https://digital-strategy.ec.europa.eu/en/library/staff-working-document-and-executive-summary-evaluation-directive-969ec-legal-protection-databases, [Last accessed 31 August 2022].

[111] European Parliament, "Directive (EU) 2016/1148 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union," July 6, 2016, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN, [Last accessed 31 August 2022].

[112] Article 3 of the NIS1.

[113] Articles 7-10 of the NIS1.

[114] Articles 11-13 of the NIS1.

3. **Supervision of critical sectors providing essential services**[115], concentrating on:
    a. Ensuring that operators of essential services take appropriate and proportionate technical and organisational measures to prevent and minimise the risks posed while notifying the authorities of incidents having a significant impact on their services.

Where personal data is involved, the provisions of the GDPR shall apply, as per Article 2 of the NIS1 Directive. The Data Protection Policies (Deliverable 3.6) address the implementation legislation introduced by the Member States.

5.7.2. NIS2 (upcoming revision)

In May 2022, the EU reached an agreement on the proposal for an updated version of the NIS Directive, which was already introduced in 2020, **adapting the respective framework to modern standards and needs of protection**, taking into consideration the evolution of technology in all sectors and the increased cyberattack risks. The proposed Directive (hereafter NIS2)[116] **extends the scope of application** to include not only public and private entities deemed essential, but also important entities, excluding only micro and small enterprises, unless they are offering public order services, under certain conditions[117].

In addition to the existing policies established by the Member States, the latter shall also ensure that **cybersecurity tools and measures sustain the general availability and integrity of the public core of the internet**[118]. At the same time, it adds the obligation for CSIRTs to **disclose vulnerabilities** in a coordinated way, reported to the European vulnerability registry maintained by ENISA[119]. It also specifies more in detail the duties of the CSIRTs, the CSIRT network, as well as the Cooperation Group established.

Moreover, Member States shall be responsible to designate competent authorities responsible for the **management of large-scale incidents and crises**, along with an adequate response plan[120]. ENISA shall also issue a biennial report on the state of the cybersecurity in the Union[121], while a peer-review system for assessing cybersecurity policies shall be established[122]. Of course, in order to demonstrate compliance, the Directive introduces the option of using cybersecurity certification schemes.[123]

5.8. AI Act

Noting the unprecedented evolution of Artificial Intelligence (AI) technologies, the European Union recognised the need to actively regulate the sector, in addition to providing mere ethics guidelines[124],

[115] Articles 14-18 of the NIS1.

[116] European Commission, "Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Measures for a High Common Level of Cybersecurity across the Union, Repealing Directive (EU) 2016/1148," December 16, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:823:FIN, [Last accessed 31 August 2022].

[117] Article 2 of the NIS2.

[118] Article 5 of the NIS2.

[119] Article 6 of the NIS2.

[120] Article 7 of the NIS2.

[121] Article 15 of the NIS2.

[122] Article 16 of the NIS2.

[123] Article 21 of the NIS2.

[124] High-Level Expert Group on Artificial Intelligence, "Ethics Guidelines for Trustworthy AI," April 8, 2019, https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai, [Last accessed 31 August 2022].

thus resulting in the first major legislation proposal in April 2021[125] with the Proposal for a Regulation laying down **harmonised rules on Artificial Intelligence (Artificial Intelligence Act)** and amending certain Union legislative acts[126]. By laying a uniform legal framework, the proposed Regulation aims at meeting the following **objectives**[127]:

1. Ensuring **AI systems' safety and compliance with existing law** on fundamental rights and EU values,
2. **Enhancing legal certainty** to foster investments and innovation initiatives in AI,
3. **Improving governance and effective enforcement** of existing fundamental rights legislation and safety requirements, and
4. **Gathering lawful, safe, and trustworthy AI applications** under a single market and preventing market fragmentation.

The term AI in the context of the Regulation is meant to incorporate a **list of software-producing techniques, including:**

(a) **Machine learning** approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;

(b) **Logic- and knowledge-based approaches**, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;

(c) **Statistical approaches**, **Bayesian estimation, search and optimisation methods**[128].

Taking into consideration the powerful impact AI can have, the Regulation distinguishes **three risk categories of AI systems**: 1) those that create an **unacceptable risk**, 2) **high-risk** applications, and 3) applications **not specifically banned** or included in the aforementioned lists.

Based on what is outlined above, the first category includes a list of inherently prohibited practices[129], namely:

a. AI that deploys subliminal techniques **beyond a person's consciousness having the potential to or actually resulting in in that person or another person physical or psychological harm**,
b. AI that **exploits any of the vulnerabilities of a specific group** of persons due to their age, physical or mental disability, in a manner that causes or is likely to cause that person or another person physical or psychological harm,
c. AI owned **by public authorities** or used on their behalf for the **evaluation or classification of the trustworthiness of natural persons** over a certain period of time based on their social

[125] Future of Life Institute (FLI), "What Is the EU AI Act?," *Artificial Intelligence Act* (blog), accessed June 17, 2022, https://artificialintelligenceact.eu/, [Last accessed 31 August 2022].

[126] European Commission, "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS COM/2021/206 Final," April 21, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206, [Last accessed 31 August 2022].

[127] Explanatory memorandum to the Proposal for the AI Act, par. 1.1.

[128] Annex I to the AI Act.

[129] Article 5 of the draft AI Act.

behaviour or known or predicted personal or personality characteristics, with the social score leading to either or both of the following:

1) **detrimental or unfavourable treatment** of certain natural persons or whole groups thereof **in social contexts which are unrelated to the contexts in which the data was originally generated or collected**,
2) **detrimental or unfavourable treatment** of certain natural persons or whole groups thereof that is **unjustified or disproportionate** to their social behaviour or its gravity,

d. **'Real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement**, **unless** and in as far as such use is strictly necessary for the targeted search for specific potential victims of crime, the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack, or the detection, localisation, identification or prosecution of a perpetrator or suspect of a serious criminal offence recognised by the Union and punishable with a sentence of at least 3 years in national orders. All practices falling within the scope of the aforementioned exceptions shall abide by the **principles of proportionality and necessity**.

The second category refers to **AI systems considered high-risk by nature** and, thus, require the establishment of a specific set of requirements. Such high-risk AI may include, but is not limited to, AI offering access to and enjoyment of essential private services and public services and benefits and the management and operation of critical infrastructure[130].

As a result, high-risk AI is subject to a **risk management system** that, through testing, shall identify and analyse any foreseeable risks, estimate and evaluate said risks, as well as adopt suitable measures to combat and/or prevent them to the highest degree possible[131]. Where training, validation and testing data sets are being deployed, they shall be subject to **appropriate data governance and management practices,** while they need to be relevant, representative, free of errors and complete[132]. The same conditions apply to the required quality management system.[133]

In addition to the above, before circulating a high-risk AI system, **adequate technical documentation** must be drafted and updated frequently, demonstrating compliance[134]. For reasons of **traceability, transparency and interpretation of output** after provision of sufficient information[135], the AI systems shall possess an automatic recording of events (logs) capabilities, including at least the period of each use, the reference database, the input data and the identification of the natural persons involved[136]. Of course, AI systems **must always permit human oversight**, achieving an appropriate level of **accuracy, robustness and cybersecurity** throughout their lifecycle[137].

At the same time, high-risk Ais are expected to have performed a **conformity assessment prior to their circulation** in the market and every time they are substantially modified, unless an exception according to Article 47 is applicable, while conformity can be further attested by certificates and the CE marking

[130] Annex III of the draft AI Act.
[131] Article 9 of the draft AI Act.
[132] Article 10 of the draft AI Act.
[133] Articles 16-19 of the draft AI Act.
[134] Article 11 of the draft AI Act.
[135] Article 13 of the draft AI Act.
[136] Article 12 of the draft AI Act.
[137] Articles 14-15 of the draft AI Act.

of conformity.[138] On that note, providers need to prepare a **written EU declaration of conformity** for each AI system they have placed in the market, thus assuming responsibility for compliance.

For **low-risk AI systems, a code of conduct scheme** is envisaged for a later point in time.

5.9. National Laws pertaining scientific use of data

European Union

The central provision of the EU legal framework on the scientific use of data can be found in **Article 89 (1) of the GDPR**, setting out the **safeguards that controllers must implement** to further process personal data for research purposes, which shall be subject to **appropriate safeguards** protecting the rights and freedoms of the data subjects. Such safeguards shall include **technical and organisational measures**, in particular in order to ensure that only the personal data necessary for the research purpose is processed, in accordance with the **principle of data minimisation** outlined in Article 5 (c) of the GDPR.

Moreover, the GDPR recommends a potential technical and organisational measure, namely pseudonymisation. As per Article 4 (3b), **pseudonymisation** is "*the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person*." Since Recital 26 asserts that **pseudonymised data is considered personal data** as long as it can be attributed to a natural person in combination with additional information, the Regulation also applies to pseudonymised data.

In spite of the above, **Member States were free to establish a more precise framework and include more specialised provisions** for the use of research data for scientific purposes. On that note, the table below includes a list of the States that have developed their own national provisions in addition to the GDPR requirements.

Country	GDPR application	National provisions on data protection and scientific research
Austria	Yes, EU Member State	Yes, Federal Act concerning the Protection of Personal Data
Belgium	Yes, EU Member State	Yes, Belgian Act of 30 July 2018 on the Protection of Natural Persons with regard to the Processing of Personal Data
Bulgaria	Yes, EU Member State	No additional provisions
Croatia	Yes, EU Member State	No additional provisions
Cyprus	Yes, EU Member State	Yes, Cypriot Law 125(I) of 2018 on The Protection of Natural Persons with regards to the Processing of Personal Data and for the Free Movement of Such Data
Czech Republic	Yes, EU Member State	Yes, Czech Act No. 110/2019 Coll. On Personal Data Processing
Denmark	Yes, EU Member State	Yes, Data Protection Act of Denmark
Estonia	Yes, EU Member State	Yes, Estonian Personal Data Protection Act 2018

[138] Articles 43-44, 49 of the draft AI Act.

Finland	Yes, EU Member State	Yes, Data Protection Act of Finland
France	Yes, EU Member State	Yes, Law n° 2018-493 of 20 June 2018 and Law n° 78-17 of 6 January 1978 for health data
Germany	Yes, EU Member State	Yes, German Federal Data Protection Act
Greece	Yes, EU Member State	Yes, Greek Law 4624/2019, implementing Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons concerning the processing of personal data, and transposition of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016, and other provisions
Hungary	Yes, EU Member State	Yes, Hungarian Act CXII of 2011 on the Right of Informational Self- Determination and on Freedom of Information
Iceland	Yes, Decision No. 154/2018 of the EEA Joint Committee	Yes, Icelandic Act 90/2018 on Privacy and Processing of Personal Data
Ireland	Yes, EU Member State	Yes, Irish Data Protection Act 2018
Italy	Yes, EU Member State	Yes, Italian Legislative decree no. 196 of 30 June 2003
Latvia	Yes, EU Member State	No additional provisions
Liechtenstein	Yes, Decision No. 154/2018 of the EEA Joint Committee	Yes, Liechtenstein Data Protection Act of 4 October 2018 and Data Protection Ordinance of 11 December 2018
Lithuania	Yes, EU Member State	No additional provisions
Luxembourg	Yes, EU Member State	Yes, Luxembourg Act of 1 August 2018 on the Organisation of the National Commission for Data Protection and Implementing the GDPR
Malta	Yes, EU Member State	Yes, Maltese CAP 586
Netherlands	Yes, EU Member State	Yes, Dutch GDPR Implementation Act
Norway	Yes, Decision No. 154/2018 of the EEA Joint Committee	Yes, Norwegian Personal Data Act of 15 June 2018 on special categories of data and criminal convictions data
Poland	Yes, EU Member State	Yes, Polish Personal Data Protection Act of 10 May 2018
Portugal	Yes, EU Member State	Yes, Portuguese Law no. 58/2019
Romania	Yes, EU Member State	Yes, Romanian Law No. 190/2018 Implementing the General Data Protection Regulation
Slovakia	Yes, EU Member State	No additional provisions
Slovenia	Yes, EU Member State	Yes, Slovenian Personal Data Protection Act
Spain	Yes, EU Member State	Yes, Spanish Organic Law 2/2018 on Data Protection and Guarantee of Digital Rights
Sweden	Yes, EU Member State	Yes, Swedish Act containing Supplementary Provisions to the EU General Data Protection Regulation (SFS 2018:218)
Switzerland	Yes, Decision No. 154/2018 of the EEA Joint Committee	Yes, Swiss Federal Act on Data Protection
UK	Not after 31 December 2020	Yes, UK General Data Protection Regulation

6. Applicable Regulations for Open Science

6.1. UNESCO Declaration

During the 40th session of UNESCO's General Conference in 2019, the need for an international standard setting instrument on Open Science became more apparent to further its Strategy on Open Access to Scientific Information and Research[139]. As a result, in 2021 UNESCO published the **Recommendation on Open Science**[140], which is meant to complement the 2017 Recommendation on Science and Scientific Research[141], taking into consideration the vital role of science and technology innovations in modern societies to combat emerging challenges.

The Recommendation starts with reinstating the term "open science", further expanding essential principles such as **academic freedom, research integrity and scientific excellence** to include **reproducibility, transparency, sharing and collaboration**. As a result, it concludes that "open science" is defined as an "*inclusive construct that combines various movements and practices aiming to make multilingual scientific knowledge openly available, accessible and reusable for everyone, to increase scientific collaborations and sharing of information for the benefits of science and society, and to open the processes of scientific knowledge creation, evaluation and communication to societal actors beyond the traditional scientific community*". As such, it involves all scientific disciplines and aspects, **building on open scientific knowledge, open science infrastructures, science communication, open engagement of societal actors and open dialogue with other knowledge systems**[142].

In particular as far as open research data is concerned, UNESCO explicitly includes **various types of data, digital and analogue data, both raw and processed, and the accompanying metadata**, as well as numerical scores, textual records, images and sounds, protocols, analysis code and workflows that can be openly used, reused, retained and redistributed. In order to meet the conditions of open research data, **it must be:**

b. **Available in a timely manner,**
c. **Through a user-friendly format,**
d. **Human and machine-readable,**
e. **Actionable,**
f. **In accordance with the principles of good data governance, stewardship, the FAIR principles,**
g. **Supported by regular curation and maintenance[143].**

Similarly, when discussing open-source software, it must meet the above requirements, along with its licensing, choosing a licen**se that grants others the right to user, access, modify, expand, study, create derivative works and share the software and its source code, design or blueprint**. Additionally, it must be **shared in openly accessible repositories**. Specifically, when opening a research process comprises

[139] UNESCO, "Open Access to Scientific Information," n.d., https://en.unesco.org/themes/open-access-scientific-information, [Last accessed 31 August 2022].

[140] UNESCO, "UNESCO Recommendation on Open Science," 2021, https://unesdoc.unesco.org/ark:/48223/pf0000379949.locale=en, [Last accessed 31 August 2022].

[141] UNESCO, "Records of the General Conference, 39th Session, Paris, 30 October-14 November 2017, v. 1: Resolutions," 2018, https://unesdoc.unesco.org/ark:/48223/pf0000260889.page=116, [Last accessed 31 August 2022].

[142] Par. 4 of the Open Science Recommendation.

[143] Par. 7(b) of the Open Science Recommendation.

of open-source code, it must be accompanied by **open data and open specifications of the environment required to compile and run it**[144].

In line with the above, open science infrastructures incorporate **all shared research infrastructures, virtual or physical, including major scientific equipment or sets of instruments, knowledge-based resources such as open access publication platforms, repositories, archives and scientific data**, current research information systems, open computational and data manipulation service infrastructures that enable collaborative and multidisciplinary data analysis and digital infrastructures. The critical components of such infrastructures can be found, among others, in **open science platforms and repositories for publications, research data and source codes, software forges and virtual research environments, and digital research services,** in particular those that allow to identify unambiguously scientific objects by persistent unique identifiers. Open innovation testbeds, also form part of the aforementioned open-source infrastructures, providing common access to physical facilities, capabilities and services[145].

Of course, open science requirements do not automatically exclude every and all **restrictions**, but if they are placed, they must be **proportionate and justified on the basis of one of the following reasons**:

1. **Human rights protection,**
2. **National security,**
3. **Confidentiality and the right to privacy,**
4. **Respect for human subjects of studies,**
5. **Leal process requirements,**
6. **The protection of public order,**
7. **The protection of intellectual property rights,**
8. **The protection of sacred and secret indigenous knowledge,**
9. **The protection of rare, threatened, and endangered species.**

Where such restrictions are placed, it is **essential to confirm whether data could still be made available after pseudonymisation or anonymisation or providing mediated access**[146].

The **principles and values of open science prescribed by UNESCO** can be summed up as follows:

[144] Par. 7(d) of the Open Science Recommendation.

[145] Par. 9 of the Open Science Recommendation.

[146] Par. 8 of the Open Science Recommendation.

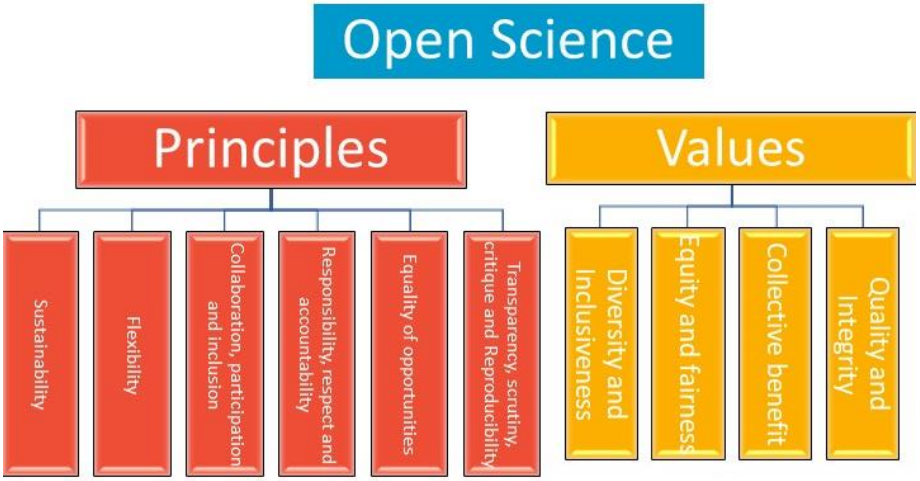


Figure 1: UNESCO Open Science Principle and Values

The tools and solutions developed by scientists and researchers based on the above ethical framework are meant to facilitate research and innovation, improving results speed, accuracy and efficiency, while enabling scientists from low and middle-income countries to utilise them in turn[147].

As per Chapter IV of the UNESCO Recommendation on Open Science, **States are to focus on seven areas in order to promote open science, namely:**

- Promotion of a **common understanding of open science**, associated benefits and challenges, as well as diverse paths to open science,
- Development of an **enabling policy environment** for open science,
- Investments in **open science infrastructures and services**,
- **Investments in human resources, training, education, digital literacy and capacity building** for open science,
- Establishment of a **culture of open science** and the provision of incentives for open science,
- Promotion of **innovative approaches for open science** at different stages of the scientific process,
- Promotion of **international and multi-stakeholder cooperation** in the context of open science and with a view to reducing digital, technological and knowledge gaps.

6.2. ESFRI

The **European Strategy Forum on Research Infrastructures (ESFRI),** formed in 2002, is a strategic instrument with the purpose of **evolving Europe's scientific integration and expanding its outreach** through the implementation of adequate policies. The Forum acts as an **informal body**, composed of representatives of national authorities responsible for political decision-making and funding of research infrastructures[148].

[147] Par. 18 of the Open Science Recommendation.

[148] European Strategy Research Forum on Research Infrastructures, "Activities and Procedural Guidelines for the European Strategy Forum on Research Infrastructures," March 2017, https://ec.europa.eu/info/sites/default/files/esfri_procedures_mandate.pdf, [Last accessed 31 August 2022]..

As anticipated, the **principles of Open Science in conjunction with the FAIR principles hold a prominent position** within the ESFRI framework, viewing Research Infrastructures as potential pillars of open science and innovation in Europe. As such, the vision of the **European Open Science Cloud** has emerged, as the **pathway to easy and rapid data sharing** among research infrastructures, enriching available data for research[149].

In that context, European Research Infrastructures are envisioned to meet the **criteria** below, which would not be possible without an Open Science framework:

i. They include and produce **high-quality data and metadata**, assuring robust quality control,
ii. They are **easy to access**,
iii. They **implement the FAIR principles**,
iv. They operate in **highly competitive international communities**[150].

The Roadmap of the ESFRI published in 2021 also emphasises the **importance of Open Science to the advancement of the European Research Area**, focusing on fostering a culture of open access to improve EU citizens' well-being and level of life, while **bridging any research gaps for scientists from all over Europe**. For this reason, federated, national or European infrastructures are expected to provide a **trusted and open space to store, share and re-use scientific data**, characterised by fast connectivity, high-capacity cloud solutions and supercomputer capability systems[151].

The above notions and requirements have been at the focus of nearly all projects developed within the ESFRI framework, while a selection of them involves exclusively the methods to further enhance open science in research sectors.

6.3. Open Data Directive

The Directive 1024/2019 on open data and the re-use of public sector information, also called the Open Data Directive[152], has been in force since June 2019 and it mainly aims at the **release of public sector data in free and open formats**. Recognising that public sector information constitutes an exceptional source of data useful for the improvement of the internal market and all economic sectors[153], it was deemed essential that said data be further utilised for research outside the public sector[154].

In particular, the Directive **applies to documents held by Member States' public sector bodies, public undertakings under certain conditions and certain research data**. On the contrary, the Directive **excludes** a number of data categories from its application[155], such as:

[149] "Conclusions of the Council of the European Union of 18 May 2018 on the European Open Science Cloud (EOSC).," May 18, 2018, https://data.consilium.europa.eu/doc/document/ST-9029-2018-INIT/en/pdf, [Last accessed 31 August 2022]..

[150] European Strategy Research Forum on Research Infrastructures, "Making Science Happen: A New Ambition for Research Infrastructures in the European Research Area - ESFRI White Paper 2020," March 2020, https://www.esfri.eu/sites/default/files/White_paper_ESFRI-final.pdf, [Last accessed 31 August 2022].

[151] European Strategy Research Forum on Research Infrastructures, "Roadmap 2021: Strategy Report on Research Infrastructures," n.d., https://roadmap2021.esfri.eu/media/1295/esfri-roadmap-2021.pdf, [Last accessed 31 August 2022].

[152] European Parliament and Council of the European Union, "Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on Open Data and the Re-Use of Public Sector Information," June 20, 2019, http://data.europa.eu/eli/dir/2019/1024/oj/eng, [Last accessed 31 August 2022].

[153] Recital 9 of the Open Data Directive.

[154] Article 3 of the Open Data Directive.

[155] Article 1 of the Open Data Directive.

(i) Documents referring to an **activity outside the scope** of a public task of public sector bodies or public undertakings as defined by law,
(ii) Documents related to activities **directly exposed to competition**,
(iii) Documents for which third parties hold **intellectual property rights**,
(iv) Documents including **sensitive data**, referring to the protection of national security (namely, State security), defence, or public security, statistical confidentiality and commercial confidentiality,
(v) Documents with restricted access for **personal data protection** reasons,
(vi) Documents **held by cultural establishments other than libraries, including university libraries, museums and archives**, and
(vii) Documents **held by specific research performing organisations and research funding organisations**, including organisations established for the transfer of research results.

The Directive lays down the **procedure for the re-use of publicly held data** as follows[156]:

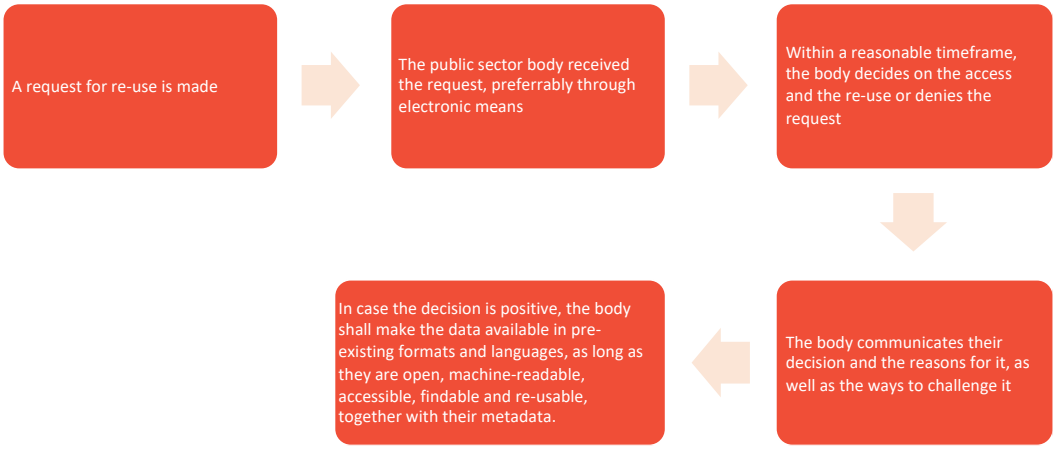


Figure 2:Procedure for the re-use of publicly held data

The public sector bodies must abide by the following **general principles**:

a. Access to the data shall be **free of charge**, based on Article 6 par. 1, with the exception of marginal costs incurred for the reproduction, provision and dissemination of documents as well as for anonymisation of personal data and measures taken to protect commercially confidential information. Nonetheless, this does not apply to public sector bodies that are required to generate revenue to cover a substantial part of their costs relating to the performance of their public tasks, libraries, including university libraries, museums, archives and public undertakings, as per par. 2 of the same article, although any charge must remain reasonable and transparent[157],
b. The conditions for the re-use of documents shall be **non-discriminatory**[158],

[156] Articles 5-6 of the Open Data Directive.
[157] Articles 6-7 of the Open Data Directive.
[158] Article 11 of the Open Data Directive.

c. Contracts or other arrangements between the public sector bodies or public undertakings holding the documents and third parties **shall not grant exclusive rights, unless that is required** to protect the public interest under certain conditions[159].

In addition to the above, when there are **high-value datasets involved, they shall be**[160]:

(a) **available free of charge**, where possible;
(b) **machine-readable**;
(c) **provided via APIs**; and
(d) **provided as a bulk download**, where relevant.

Such **high-value datasets**, according to par. 2 of Article 14, are characterised by the potential to "**generate *significant socioeconomic or environmental benefits and innovative services, to benefit a high number of users***, *in particular SMEs, to assist in generating revenues; and* to *be combined with other datasets".* Annex I of the Directive includes a list of thematic categories of high-value datasets, namely referring to the geospatial data, earth observation and environmental data, meteorological data, statistics, companies and company ownership and mobility data.

The Directive also explicitly mentions that the **availability of research data** shall be heavily supported by the Member States, adopting **open access policies**, in accordance with the **"open by default"** and the **FAIR principles**, always **respecting intellectual property rights, personal data, security and legitimate interests**[161]. As such, "*research data shall be re-usable for commercial or non-commercial purposes, insofar as they are publicly funded and researchers, research performing organisations or research funding organisations have already made them publicly available through an institutional or subject-based repository*".

6.4. Copyright Directive

Following the initial EU effort to harmonise copyright in the emergence of the digital era in the beginning of the millennium, the **Directive on Copyright in the Digital Single Market**[162] was adopted, aiming at establishing a copyright framework adapted to the needs of modern society and the updated goals of the Union for the internal market[163]. As such, the Directive **balances copyright related rights and exceptions mainly deriving from open science requirements for scientific research purposes**[164].

In particular, the Directive, which was to be transposed by 7 June 2021[165], **maintains in force the exclusive reproduction rights established in Article 2 of Directive 2001/29/EC[166], as well as in Articles**

[159] Article 12 of the Open Data Directive.

[160] Article 14 of the Open Data Directive.

[161] Article 10 of the Open Data Directive.

[162] European Commission, "Directive (EU) 2019/790 of the European Parliament and of the Council on Copyright and Related Rights in the Digital Single Market and Amending Directives 96/9/EC and 2001/29/EC" (2019), https://eur-lex.europa.eu/eli/dir/2019/790/oj, [Last accessed 31 August 2022].

[163] Recital 2-3 of the Copyright Directive.

[164] Article 1 of the Copyright Directive.

[165] Article 29 of the Copyright Directive.

[166] "Directive 2001/29/EC of the European Parliament and of the Council on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society" (2001), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32001L0029, [Last accessed 31 August 2022].

5 and 7 of the Database Directive mentioned above. Nonetheless, it provides for a **series of exceptions** based on the following:

- **Text and data mining for the purposes of scientific research**, for reproductions and extractions made by research organisations and cultural heritage institutions, maintain an appropriate level of security and integrity[167],
- **Use of works and other subject matter in digital and cross-border teaching activities**, by an educational establishment through a secure electronic environment to pupils/students and teaching staff[168],
- **Purposes of preservation of cultural heritage** by cultural heritage institutions[169].

The Directive also includes provisions aiming at **improving licensing** while ensuring wide access to content, namely in the following cases:

- In the case of **out-of-commerce works, a collective management organisation**, in accordance with its mandates from rightholders, may conclude a **non-exclusive licence for non-commercial purposes with a cultural heritage institution** for the use of the works that are permanently in the collection of the institution in any Member State, as long as the rightholders are sufficiently protected[170],
- The performance of a **licensing agreement for the exploitation of works or other subject matters by collective management organisations** even when rightholders have not authorised that collective management organisation to represent them by way of assignment, licence or any other contractual arrangement or it is presumed to represent the rightholders not authorised the organisation[171],
- The **use of protected content by online content-sharing service providers**, after obtaining authorisation by the rightholders, unless the relevant conditions for unauthorised use are met[172].

Where authors and performers license or transfer their exclusive rights for the exploitation of their works or other subject matter, they are entitled to receive **appropriate and proportionate remuneration**[173]. At the same time, they shall be **informed on a regular basis and, at least, annually, of the exploitation of their works and performances** from the parties to whom they have licensed or transferred their rights, or their successors in title, in particular as regards modes of exploitation, all revenues generated and remuneration due, in accordance with transparency requirements[174]. Any **license or authorisation shall be freely revoked after a reasonable time** following the conclusion of the licence or the transfer of the rights[175].

[167] Article 3 of the Copyright Directive.
[168] Article 5 of the Copyright Directive.
[169] Article 6 of the Copyright Directive.
[170] Articles 8-9 of the Copyright Directive.
[171] Article 12 of the Copyright Directive.
[172] Article 17 of the Copyright Directive.
[173] Article 18 of the Copyright Directive.
[174] Article 19 of the Copyright Directive.
[175] Article 22 of the Copyright Directive.

7. Legal Risks

Having reviewed the relevant legislation and guidelines provided on the main legal and ethical requirements of interest for the SLICES project, a number of potentially risk incurring points have been identified, that can be summed up as follows:

7.1. Data management and security protocols

It is essential that a robust internal data management protocol is established and implemented. Based on these internal protocols, a **clear organisational structure** shall be defined, specifying **which employees and staff have access to which data** inserted, stored and potentially processed, while ensuring that **unauthorised personnel shall not have access** to the data.

Similarly, the internal-use protocols shall in detail describe the **security measures** in place **to prevent not only unauthorised access, but also the loss, destruction and/or alteration** of data due to technical problems. Said security measures shall include **specific security incidents management steps**, providing not only for the back-up of data, but also the **exact procedures that personnel must follow**.

7.2. Cybersecurity

In addition to the above, a cybersecurity protocol must be set in place to protect the data and the testbeds from potential cybersecurity threats. The transition to online and cloud-based solutions, such as testbeds, providing enhanced interconnectivity and AI technologies has been marked by a **drastic increase in cybersecurity threats**, not only in terms of numbers but also in the context of methods used and level of sophistication[176].

In view of that, it is essential that the cybersecurity measures implemented do not only guarantee protection from any attacks at that given moment but that they are **constantly kept up to date**, to prevent future attacks as well. For this reason, the cybersecurity protocol shall be viewed as a living instrument, which shall be reviewed frequently.

7.3. System maintenance and updates

Apart from external threats that may result in liability disputes, it is also vital to consider the **frequency of maintenance, upgrade and update actions,** distinguishing between **scheduled maintenance** services and **urgent maintenance** that shall be conducted in response to a specific issue arising at a given time.

Of course, **users shall be notified in advance** of scheduled maintenance and updates in the system, specifically of the date and time carried out, so as to avoid them being prevented from using the testbeds effectively and without problems.

7.4. Terms and conditions / adequate use policy

A **detailed Terms and Conditions policy** needs to be drafted in order to protect the project from it being used in illegal or otherwise undesired manners. Said policy must specifically describe which users

[176] European Union Agency for Cybersecurity., *ENISA Threat Landscape 2021: April 2020 to Mid-July 2021.* (LU: Publications Office, 2021), https://data.europa.eu/doi/10.2824/324797, [Last accessed 31 August 2022].

are eligible to use the platform, for which purposes, the allowed and forbidden actions, as well as any costs.

Additionally, it should provide the requirements that they must meet to use the platform along with any documentation required for their authentication and unhindered use. The Terms and Conditions Policy shall also include the cases in which a more specialised contract with the users shall be signed.

7.5. Cookies and privacy policy

An **effective cookie and privacy policy** shall be drafted and provided to the users upon their entry to the platform. The platform must include the details of the data that is required for registration, authentication etc, as well as the data that it shall collect on its own.

Users must have the **option to consent** to the collection and processing of their data, as well as the **option to opt out** where that is possible. Any data collected and/or processed needs to be necessary to achieve the legal purposes that shall be prescribed, mainly taking into consideration the requirements of consent and the fulfilment of a legal contract.

7.6. Liability issues and potential dispute settlement

Last but not least, both users and platform/service providers need to be provided a **thorough explanation of their rights** in case any issues arise. Apart from the right to revoke consent, the right to be forgotten and the right of rectification, that play a central role in this, users need to be aware of **liability issues** in case their personal data or the data resulting from their use of the testbed is irretrievably lost, destroyed or altered.

In this case, it should be described **how they can address these matters in the context of the SLICES project, national authorities, extrajudicial mechanisms, and, finally, court jurisdiction.**

8. Guidelines and Recommendations

The following section consists of a **series of guidelines and recommendations** in order to not only combat the legal risks discussed above but also to further progress the project from a legal and ethical standpoint. Said guidelines and recommendations **expand from administrative procedures to the organisational structure, compliance activities and the expected data protection policy.**

8.1. Administrative Procedures

The administrative procedures suggested shall involve the steps that need to be taken on an internal level to ensure the proper functioning of the project. In particular, it is necessary that the following **questions are considered so as to design, draft and implement the internal policies and procedures required.**

Who will be authorised to access the data collected, processed and stored, both digitally and physically?	It is essential to determine and clearly define access rights to the electronic files as well as the servers' facility. Access rights is an essential part of a safety policy, as it not only provides clarity as to

	each person's position and obligations, but it also protects the totality of the Consortium from unwanted liability claims.
What are the user support activities, products or services that shall be developed (e.g., Data back-ups frequency, AI virtual assistant etc.)?	As in all digital platforms, it is likely that users face difficulties, problems or may require general assistance to utilise the platform. A trustworthy solution needs to predict and respond to any issues experimenters may face when using the testbeds. Such measures can be two-fold; on one hand, they may involve frequent back-ups of the experiment' progress or similar measures in order to prevent loss of data that could be detrimental in case a technical error or an error on the experimenter's side arises. Of course, it is always important to determine the duration of retention of such data to comply with the relevant legislative prerequisites. On the other hand, such user support systems may include technical support and assistance, either in the form of an actual natural person responding to requests and demands for assistance or a virtual assistance solution based on AI. If such support includes a natural person, it should be ensured that they possess sufficient knowledge of the platform's functioning as well as of general technical issues in order to be able to respond to such requests. If any request for access to data is performed or a notification of a security or technical error, it must be made sure that they have authorisation to perform the acts required and they are duly informed of the procedures of notification of breaches to the DPO. If a virtual assistant is chosen, there is an additional set of safeguards that must be placed in accordance with the requirements for an ethical and legal AI system, that will not only effectively assist the user, but will also complete said task with respect to personal data and human rights.
Will there be users' training involved? If so, what exactly will such training contain (e.g., person-to-person training, demos, instructions, etc.)?	Given that not all potential users of the platform may be familiarised with such an environment, as well as the innovative elements that the testbeds intend to have, it is advised to incorporate various training materials in the project's website. Such material may include a video and/or written demonstration of how to use the testbed and its various features and possibilities, a clear set of instructions or even test users' case. In the event that actual test user case shall be utilised, it is important to ensure that any personal data belonging either to that particular user or the test experiment at hand shall be protected. This means that the user's informed consent needs to be obtained for every act that shall be involved, including video and voice feed. The user needs to comprehend exactly how this data shall be used, where it will be displayed, who shall have access to it and the relevant duration.

	It is additionally possible to incorporate training in person where that may be requested. In this case, it is essential to determine the precise conditions for the training, the need for a training contract, its duration and length of training, as well as whether said service shall be conducted for a fee.
In terms of publications of researchers' results, will it be required that the use of the SLICES testbeds be mentioned and credited?	As the purpose of the testbeds is to provide a solid environment for researchers and scientists to use in their experiments, fostering innovation and technological progress, the researchers' utilising the platform may proceed to a publication of the results of their experiments. In such an event, it is important to define whether mention of the particular testbeds is required. In the affirmative, it is necessary that such requirement is clearly mentioned in the relevant terms of use of the platform in a way that is comprehensible and noticeable by the users prior to the registration in the platform. A template may also be used to ensure proper crediting of the testbeds' use and potential. The relevant terms shall include any liability provisions in case the crediting requirement is not met
Will any of the testbeds features or services be provided for a fee?	If the totality of the testbeds' features, possibilities and services are provided free of any charge, there are no additional terms that need to be included. However, if there are particular features or services that shall be provided for a fee, it is essential that this is clear prior to a users' registration, in accordance with transparency requirements. Moreover, the payment methods shall be mentioned, while a safe and secure environment shall be used for payments. A refund policy shall also need to be included, along with a proper dispute settlement framework.
Will the testbeds / SLICES platform provide for the possibility for multiple users to work simultaneously together on the same project?	If that possibility is provided, it shall be essential to maintain log-in and editing records to avoid loss, destruction and alteration of data from one of the parties involved. The system also needs to be capable from a technical point of view to support multiple access and editing, whether simultaneously or in turns. It shall be clearly stated that the testbeds bear no responsibility for the conclusion, substantive structuring and execution of such a user-to-user collaboration and such collaboration shall be governed by the users own separate relationship. The testbeds shall hold no liability in case the user-to-user agreement is breached by any of the parties.
Will there be a long-term preservation plan for selected data produced through the testbeds?	
What is the information that metadata shall include?	It is generally advised that metadata includes a minimum content that shall render them sufficient and identifiable respecting the FAIR principles. Such minimum content may include: ➢ The experiment's title,

	➢ The author/contributor's name(s), ➢ The author/contributor's identification number(s), ➢ An abstract, shortly describing the content of the experiment, ➢ Keywords that may be used to identify the subject matter of the experiment, ➢ The type of data Licence used, if any, ➢ The data's identifier, usually the Digital Object Identifiers (DOI), ➢ The date of publication, ➢ The file's version, ➢ The institution(s) affiliated with the authors or contributors, ➢ Funder(s), where a grant has been awarded.
Will the testbeds be available for non-EU based researchers and experimenters?	In case, access is provided to non-EU based researchers, it may be possible that additional safeguards be placed in terms of personal data protection, as well as the quality of the data imported.
Will the users also involve public sector bodies?	It is likely that for certain public sector bodies a specialised procedure needs to be followed for them to use the platform, including a specialised contract. It is additionally possible that documentation may be requested to demonstrate the testbeds legal compliance, technical characteristics and effectiveness. In order to foster this level of trust, certification may be used where possible, for instance to demonstrate compliance with data protection requirements.
What personal data shall be collected on the users? How will authentication take place?	It is crucial that users' personal data is protected at all times, according to the legislation applicable, and, in particular, in accordance with the GDPR. The data collected on the user may not be more that what is required to ensure proper use of the testbeds and conducting the experiment. In case further authentication is required, for instance proving representation of a certain legal entity, said authentication documentation may not supersede the necessary for the authentication purposes and may not be retained longer than required.
Will there be Open Calls for experiments involved?	In the affirmative, clear, transparent and non-discriminatory selection criteria may be defined. At the same time, a template for the open call contract may be designed to facilitate such transactions, containing all required terms and conditions.

8.2. Organisational Structure

8.2.1. DPO

In view of the importance of the Data Protection Officer's (DPO) role in the data governance systems, it is essential that certain measures are taken to ensure compliance. A first step towards that is the **creation and utilisation of a separate email address** for the DPO, dpo-slices-ds@npafi.org, that both the Consortium, as well as users are able to contact. This email address, as per Deliverable SLICES-DS D7.1, will be linked to four members of the Consortium to increase efficiency.

As already explained in previous deliverables, the project's DPO, i.e. Panayiotis Andreou, shall also carry out **risk assessments** on a regular basis to identify potential risks related to the collection and processing of personal data. On that note, it is crucial to define precisely the personal data that shall be collected and processed.

For instance, if the Consortium decides that they shall allow for **experimenters to enter personal data in their experiments**, the testbeds shall also act as a processor. In this case, the project's DPO shall be responsible for monitoring the processing agreements that must be signed with the experimenters, as well as work in tandem with the experimenters' DPO to determine the legality of the personal data collected to be processed (e.g., If consent requirements have been met, the existence of other lawful bases, safeguards in place etc).

In view of the above, **experimenters shall be required upon registration of their experiment to declare whether they intend to use personal data**. In the case that **such action shall be allowed**, it is necessary to proceed to the following:

- ➔ The experimenter shall declare that they are the Data Controller for all data involved in their experiment, and they will be required to prove compliance with all the relevant requirements of the GDPR.
- ➔ The experimenter will need to declare the categories of personal data they intend to use, so as to adjust the level of safeguards required.
- ➔ A proper Data Processing Agreement shall be signed.

In the case the Consortium decides **not to allow the use of personal data**, excluding anonymised data that cannot be identified, the experimenter shall be required to guarantee that no such data will be used for their experiment and assume complete responsibility for any violations of the above. All documents provided regarding personal data usage, or its lack thereof shall be stored to the personal **data register held by the project's DPO**.

Finally, the DPO shall be responsible to **identify the data sets collected** by the testbeds, **record the documentation and information provided** by the experimenters for authentication purposes and personal data usage, as well as their own DPOs where applicable, and **ensure that the project's data protection and privacy policy displayed on its website remains updated**.

8.2.2. Compliance Office

In order to ensure that the legal requirements regarding the operation of the testbeds are met at all times, it has been decided that a Compliance Office shall be established. It is recommended that **members to the compliance office possess sufficient knowledge, training and experience** in compliance and legal activities. They shall also have a **deep understanding of the organisation's functions, activities and organisational structure**, so as to be able to complete their tasks successfully.

Among its **main responsibilities** shall lie:

- The implementation and monitoring of an **effective legal compliance policy**,
- The **assessment** on a regular basis of the adherence to compliance requirements,
- The **audit** of the testbeds' activity to identify potential vulnerabilities, risks and threats,
- The **management of regulatory risks**,
- The **update** of the existing policy to match the latest regulations and compliance requirements,

- The **performance of staff training activities** to effectively communicate SLICES' ethical principles and legal policies,
- The **coordination** of actions as a **single point of contact** among the various testbed actors.

The activity and documents produced by the Compliance Office shall be subject to the **highest level of autonomy and impartiality** in order to reflect the true status within SLICES, identify potential risks and effectively prevent or counteract them. **Transparency and accountability** are of utmost importance for the SLICES project.

The Compliance Office shall also be liable to **collect documentation on and maintain a record of compliance**, producing relevant reports and recommendations. Thus, one of the first responsibilities of the Compliance Office once officially established shall be precisely this collection of documentation on compliance, along with a report reviewing existing policies thus far and potential mitigation measures for any identified risks. Deliverables already on these matters may serve as the basis for such initial review. Of course, the record of compliance shall be updated frequently to reflect the SLICES ongoing progress.

In view of the importance of the Compliance Office for the project's operation, it is suggested that such a compliance office is established the as **soon as possible**.

8.2.3. Single entry point as a legal entity

It has already been determined that the incorporation of a legal entity as a single-entry point is the most suitable course of action moving forward with the project for a number of reasons. First of all, a single legal entity shall provide a **larger degree of organisational simplicity**, taking into consideration that **representation of the SLICES project shall be facilitated**. Furthermore, entry into contracts, contractual obligations, as well as any applications or requests will be **more easily channelled through a single legal entity.**

For these reasons, it has been agreed upon that a **legal entity shall be incorporated**, assuming **either the form of an AISBL, International Non-Profit Organisation (INPA) under the Belgian law, or an ERIC - European Research Infrastructure Consortium.** The table below consists of a side-by-side comparison of the two, that have already been included in previous deliverables.

Type	AISBL, International Non-Profit Organisation (INPA) under the Belgian law	ERIC - European Research Infrastructure Consortium
Overview	The organisation is created with a minimum of 3 members, not-for-profit and not pursuing commercial or industrial activities and does not seek to provide material benefit to its members. AISBL can develop economic activities but on an ancillary basis.	ERICs are created by Council Regulation (EC) No 723/2009 of 25 June 2009 on the Community legal framework for a European Research Infrastructure Consortium (ERIC). Legal entity created by decision of the European Commission. Its main mission is to establish and develop a research infrastructure on a non-economic basis.
Founding Members	Individuals, private and public legal entities.	States or inter-governmental organisations

Legal Personality	Yes	Yes
Corporate structure and governance	Flexible, but mandatory to clearly determine the scope and allocation of powers in the Articles of Association Minimum: • General Management Body (usually composed of the members) • Executive Body	Minimum: Assembly of members AND a director OR a board of directors
Membership	Individuals and legal entities (both for the general management body and the executive body).	An ERIC must have at least one member state and 2 other countries (member states or associated countries as members). The following entities may become members of an ERIC: member states, associated countries, third countries other than associated countries and intergovernmental organisations.
Possibility to transform the structure into ERIC	Conversion to an ERIC is not provided for in the ERIC regulations. This seems theoretically possible if INPA has no members other than those authorised as members of an ERIC (EU Member States, associated countries, third countries and intergovernmental organisations) and, of course, subject to approval by the European Commission.	-
Fiduciary Duties	No fiduciary duty (but duty of "good management")	According to the ERIC regulation, an ERIC is liable for its debts. It has no immunity from seizure of its assets in the event of forced debt collection or insolvency proceedings. Proceedings are generally governed by the law of the registered office.
State supervision	No supervisory authority. The prosecutor has the right to prosecute an AISBL and request dissolution in 4 cases: (1) The use of the means or income of the AISBL for purposes other than those for which the AISBL was established; (2) Insolvency; (3) Lack of management; (4) Serious violations of the Statutes, the law or public order.	Member states and associated countries must jointly hold the majority of voting rights at the GA.

Audit	Mandatory when AISBL: (1) has an average of more than 100 full-time equivalent employees; or (2) meets or exceeds 2 of the following thresholds: (i) 50 full-time employees; (ii) total revenues of EUR 7.3 million; (iii) balance sheet total of EUR 3.65 million.	An ERIC must produce an annual activity report containing, in particular, the scientific, operational and financial aspects of its activities. An ERIC is subject to the requirements of the applicable law with respect to the preparation, filing, auditing and publication of accounts.
Tax exemption	AISBL are not subject to income tax, but to corporate income tax. In particular: • 27% on royalties (but possible to avoid if the agreement is structured in such a way that the royalties are in fact contributions to a research project undertaken by the entity); • 27% on income from portfolio investments (15% on dividends in some cases); • 0.17% of total gross assets; • 21% VAT if economic activities are undertaken in Belgium. No prior approval is required.	Under the guidelines, exemptions may thus apply to goods or services acquired by the ERIC or its members for the official use of an ERIC, subject to stated limitations and conditions. The definition of the scope, limits and conditions of the exemption may be part of the Statutes or be the subject of a separate agreement between the members or with the host State.
Labour Law	Rather strict	Strict Article 24

Taking the above into consideration, in order to facilitate the choice among the two legal vehicles and given that their **main differences lie in the level of autonomy and the financial implications**, it is important to distinguish which features are of greater significance to the Consortium.

More specifically, the **ERIC is defined by a stricter organisational and management structure**, as it must include at least one Member State among its founding members. As such and taking into consideration the fact that the m**ajority of voting rights must lie with the Member States and associated countries** involved, it is evident that the **autonomy** of the legal entity is significantly **restricted** as it is subject to national supervision. Depending on the **level of bureaucracy** in the countries involved, such a legal entity could be facing **delays** and even **constant audits** of its activities.

On the other hand, the **AISBL** is not bound by any obligation to involve national authorities and is, thus, **more agile in terms of composition, as well as monitoring and auditing obligations**. Of course, it must still meet all legal requirements, but it is not dependent on constant procedures outside of its own control and regulation. In fact, it is subject to external audit only if its total revenue is of great height.

In contrast to the above, **tax and financial matters governing ERICs can be more beneficial** depending on the agreements between the Consortium and the Member States and associated countries involved. In fact, if the legal entity is principally established in a country with a highly advantageous regime around taxes, income deriving from its activity could entirely be exempt.

On the contrary, the **AISBL, governed by Belgian law, has an already-defined tax regime** for such companies and its income is subject to corporate income tax, which can be quite elevated in the case of royalties, dividends and activities undertaken in Belgium.

All in all, the Consortium's choice lies in **whether autonomy is preferred over possible financial benefits or vice versa.**

8.3. Compliance Activities

Similarly, in order to trace the required measures to ensure legal compliance, it is recommended that the **following points are addressed and clarified**. On the basis of the answers provided, a clearer set of the steps to be taken shall be defined.

1. ***What shall be the exact Data Quality Management (DQM) tools developed as per the Data Management Plan described in deliverable SLICES DS D4.1?***

2. ***What shall be the final tools used towards real time data analytics?***

3. ***What shall be the exact procedure to perform the necessary metadata quality controls?***

4. ***How will the sharing of metadata be made possible?***

   Since it is required by the FAIR principles that metadata is also accessible and transferrable, it is essential to establish the precise procedure of sharing metadata for legitimate purposes. These measures shall ensure that any personal data is sufficiently protected by the relevant technical and organisational measures, without hindering the actual transferability.

5. ***What shall be the final metadata format used to facilitate interoperability?***

6. ***Will experimenters be able to input personal and/or sensitive data to conduct their experiments?***

   If experimenters are allowed to input personal and/or sensitive data as part of their experiment, it shall be necessary to ensure that appropriate safeguards are placed. In this case, the testbeds shall act as a data processor, for which a data processing agreement shall be required, describing in a precise and transparent way the conditions of the processing, as well as the high level of security standards implemented by the testbeds. A certification of the processing activities is a useful tool to ensure data processing compliance and enhance trust in the testbeds.

   If no personal and/or sensitive data will be permitted, it is recommended that the experimenters sign a declaration guaranteeing that they shall respect the requirement. It would also be beneficial if additional safeguards to that direction are placed, as well as a procedure for third parties to report violation of the no-personal-data term and its rapid resolution. In this way, they shall uptake the responsibility of abiding by the terms of the testbeds and the Consortium shall avoid any and all liability towards data subjects whose data may have been used in violation of the testbeds' terms.

7. ***Will experimenters be able to transfer the data? If so, who shall bear the associated costs?***

In accordance with ethical research requirements, as well as the latest EU legislation, the experiment data shall be easily transferable to other platforms of similar nature and capabilities. Nonetheless, this procedure bears a cost and, thus, require clarification and explicit mention if the experimenter shall bear said cost, without it being disproportionate.

8. ***How will ownership of the data be regulated? Who shall be deemed the owner of the data that will be able to manage them and secure intellectual property rights?***

This clarification is particularly important in case multiple users' contribution to the same project is allowed. In particular, it should be included in the form upon registration the person, natural or legal, that shall bear ownership of the data inserted in the testbeds, as well as the data finally produced. This shall ensure that the Consortium will under any circumstances be liable to intervene in ownership disputes among its users.

9. It is essential that the ***terms and conditions*** for the use of the platform are laid out in a clear and transparent manner. Such terms may indicatively include the following points:
    a. Complete and transparent information about the facilities, capabilities and services provided by the testbeds.
    b. Clear definition of contractual relationships and organisational structure within the legal entity that shall be created.
    c. User personal information and authorisation verification requirements, as well as the retention period of such information.
    d. Obligations of the users in the context of personal data protection, intellectual property rights and respect of legal obligations and requirements.
    e. Obligation of users to notify the operator of malfunctions and other errors.
    f. Acceptable usage of the platform (use for legitimate purposes, responsible use of resources, responsibility of passwords, no illegal or inappropriate material, respect of licensing).
    g. Copyright misuse disclaimer in case intellectual property rights are breached by the users of the testbeds.
    h. Confidentiality requirements and data protection policy.
    i. Health, safety and environment rules, respecting the sustainability principle.
    j. Liability and dispute settlement in case any of the terms are violated.

10. ***What additional safeguards will be set for dual-use items? Who will be responsible for complying with the necessary requirements for dual-use items?***

Since the testbeds provide an excellent environment for the performance of various experiments, it is crucial to consider the possibility that these may involve dual-use items, that may be used for military or other similar purposes. It is, therefore, recommended to include a declaration by the experimenters that they bear responsibility for the experiment they are conducting, as well as meeting the legal requirements laid out for the case of dual-use items.

8.4. Data Protection Policy

Taking into account the central role of personal data protection, it is essential that adequate policies are developed to ensure conformity with the legal requirements and enhance trust in SLICES' operations. The proposed Data Protection Policies are extensively analysed in the Deliverable SLICES-DS D3.6 and can be summarised to include the following main points:

a. A data protection by design and by default approach,
b. Carrying out a personal data processing mapping,
c. The establishment of a network of DPOs led by the project's DPO, i.e. Mandat International,
d. The establishment of a Compliance Office,
e. The performance of a DPIA and Risk assessments where necessary,
f. The performance of regular monitoring and compliance assessments,
g. A consent management procedure and methodology,
h. Adequate security measures,
i. A proper procedure and methodology to ensure secure cross-border and international data transfers,
j. The design of a web interface and cookie policy, and
k. The consideration of license policies.

The above policies are intended to be regularly reviewed and updated to ensure that they remain necessary, up to date with the latest regulatory requirements and effective to ensure personal data protection.

9. Conclusion

9.1. Main Takeaways

As has been established, SLICES is a **multifaceted project** that requires **careful legal planning in order to design, establish and implement those policies, procedures and processes that are more suitable to ensure legal compliance, prevent liabilities and inspire trust and confidence** in its operations.

Given the project's intricate and innovative nature, it is anticipated that **a number of legal risks may emerge,** involving either data management and security protocols, cybersecurity, the system's maintenance and updates, as well as the policies established, in particular referring to the cookies and privacy, as well as the terms and conditions. Of course, in the case of liability issues, it is required that an effective dispute settlement mechanism has been established so as to facilitate their rapid resolution.

Similarly, the **network of DPOs, led by the project's DPO, and the Compliance Office hold a prominent position in the prevention and management of potential legal risks**, monitoring and ensuring compliance during all of the project's phases.

The **establishment of a single legal entity** that shall encompass all SLICES activities is also an important step toward a simplified approach regarding legal policies, the project's representation and request management. Determining the appropriate type of legal entity for SLICES can be considered of pivotal importance for the future development of the project and the design of its policies and procedures.

Overall, it is deemed **essential to define the possibilities and limitations of the systems, as well as the exact rights and obligations of each party involved, including experimenters**. Such a clearly defined scope of action will maintain the likelihood of legal risks to a minimum, as roles are explicitly allocated and each party is aware of their rights and responsibilities, as well as of the consequences in case of non-conformity.

9.2. Actions for SLICES-SC and SLICES-PP

It has been confirmed that the potential legal risks go well beyond the predictable personal data protection implications, albeit a significant part, and, therefore, need to be diligently considered. Even though relevant regulations and legal provisions may be updated or amended along SLICES evolution, the outcomes of the present deliverable remain relevant for future endeavours and need to be taken into account along each step forward. Every SLICES-related project should base its legal structure on the present findings and further adapt them to the needs of each task and the project's level of maturity.

Annex I – National Laws on the Scientific Use of Data

Austria

In Austria, the legislative instrument applying to privacy-related issues, along with the GDPR, is the **Federal Act concerning the Protection of Personal Data (hereafter DSG)**.

In particular, as far as scientific use of data is concerned, Section 7 of the DSG governs **special provisions for the processing of personal data for research purposes**. First of all, section 7 (1) of the DSG distinguishes the processing that is not intended to result in a personalised outcome **permitting processing of personal data that are publicly accessible or lawfully collected for legitimate purposes or data that has been pseudonymised.**

All processing activities for research purposes that do not fall under the above section 7 (1) require one of the following bases:

i. A **specific legal provision** allowing the processing of personal data, or
ii. The **consent** of the data subject, or
iii. A **permit by the Austrian Data Protection Authority**.

Moreover, for the processing of special categories of personal data, it is necessary that an **important public interest** exists, that shall be met through the realisation of the research project. In this case, the data controller must ensure that **personal data is processed only by persons subject to a legal duty of confidentiality concerning the subject matter of the research or whose reliability in this respect is otherwise made credible**.

Finally, even where the processing is permitted in a form that allows the identification of data subjects, the **personal data shall be encrypted** so that the data subjects are no longer identifiable if specific phases of research can be performed with pseudonymised data. In all cases, personal data shall be rendered unidentifiable as soon as it is no longer necessary for the research purposes for which they were acquired.

Belgium

Title 4 of the Act of 30 July 2018 on the Protection of Natural Persons with regard to the Processing of Personal data (hereafter **Belgian DPA**) governs the processing of personal data for research purposes. It sets out a series of **exceptions to certain data subjects' rights when they could threaten or render impossible or seriously impair the achievement of the research purposes** while defining the **necessary safeguards** that must be taken into account in such cases. Such safeguards consist of the following:

- The requirement to **appoint a DPO** if the processing of the personal data is likely to result in a high risk;
- The requirement to add specific additional information to the **register of processing activities**, including the justification of the use of the data, the reasons why the exercise of the rights is likely to lead to the non-fulfilment of the purpose or its serious harm, the agreement concluded between the new and the original data controller or the notification concerning the data collection;
- If the controller processes sensitive data, then a **data protection impact assessment** should be included.

Moreover, **where personal data are obtained directly from the data subject**, Article 193 of the DPA requires to provide **additional information to the data subject**, notably on whether or not the personal data will be anonymised and the reasons why the data subject's rights threaten the achievement of the relevant purposes.

On the other hand, **when personal data is not obtained directly from the data subject,** the Belgian DPA demands that the controller concludes an **agreement with the original controller** to process the personal data, which shall contain the contact details of the original controller and of the new controller, and the reasons why the data subject's rights threaten the achievement of the relevant purposes. If the **data controller is exempt from concluding an agreement**, then he shall give a **notification to the original controller of such exemption**, which shall contain the reasons why the data subject's rights threaten the relevant purposes.

Additionally, the Belgian DPA establishes several **anonymisation and pseudonymisation requirements** for processing the data for research purposes. First of all, the data controller is required to process anonymous data, and if that is not possible, to process pseudonymised data. Only where neither is possible shall the controller use non-pseudonymised data. Moreover, **when the data controller further processes personal data for research purposes, that was collected for a different purpose**, then the personal data shall be anonymised or pseudonymised before further processing.

The DPA also distinguishes between the concepts of "**communication of data**", i.e., the communication of data to an identified third party, and "**dissemination of data**", i.e., the disclosure of data without identifying the relevant third party, and stipulates **separate requirements and safeguards for each situation**.

Whenever the processing of personal data for research purposes combines several original processing activities, the **controller of the original processing shall anonymise or pseudonymise data before communicating them to the controller of the further processing**. The same provision applies when the processing combines several original processing activities, of which at least one concerns sensitive data.

Finally, Article 205 of the Belgian DPA allows the dissemination of non-pseudonymised data only if one of the required conditions is met, namely when the data subject provides consent, when the data were made public by the data subject, if the data is closely linked to the public or historical nature of the data subject, or the data is closely linked to the public or historical nature of facts in which the data subject was involved.

Article 207 of the Belgian DPA states that the **data controller who communicates non-pseudonymised data to an identified third party shall in case of data breach ensure that the identified third party is unable to reproduce the data communicated**, especially where it concerns personal data as referred in Articles 9.1 and 10 of the GDPR, or the agreement between the controller of the original processing and the controller of the further processing forbids it, or if such reproduction may compromise the safety of the data subject.

Bulgaria

There are no deviations from the GDPR in the Bulgarian legislation.

Croatia

The Act contains no specific provisions on the processing of personal data for scientific and historical research purposes.

Cyprus

Under Article 31 of Law 125(I) of 2018 on the Protection of Natural Persons with regards to the Processing of Personal Data and for the Free Movement of Such Data, **the processing carried out by a controller or processor for scientific purposes or historical research excludes the use of personal data with the purpose of making a decision, which produces legal effects concerning the data subject or significantly affects it in a similar way.**[177]

Additionally, it provides a **list**[178] **of the types of data processing that require a data protection impact assessment** under Article 35 (4) of the GDPR, including certain research and scientific purposes including health data, CCTV systems, profiling, new technologies and biometric and genetic data.

(Available in English)

Czech Republic

Act No. 110/2019 Coll. On Personal Data Processing (hereafter **Czech Act**) implements the GDPR in the Czech Republic and sets out **additional requirements for data processing for scientifical and historical research purposes.**

Under Section 16 of the Act, the data controller or processor, when processing personal data for the purpose of historical or scientifical research, shall comply with specific measures, which may include:

- **Technical and organisational measures** aimed at a consistent application of the obligation pursuant to Art. 5 (1)(c) of the GDPR;
- **Logging of at least all operations of collection, entering, alteration and erasure of personal data**, which will make it possible to determine and verify the identity of the person performing the operation, and **retaining such records for a period of at least 2 years** from the date of the operation;
- Provision of **information to persons who process personal data concerning their obligations** in the area of personal data protection;
- **Designation of a DPO;**
- Special **limitation of access** to personal data at the controller or processor,
- **Pseudonymisation** of personal data;
- **Encryption** of personal data;
- Measures for ensuring **permanent confidentiality, integrity, availability and resilience** of processing systems and services;
- Measures enabling **restoration of the availability of and timely access to personal data** in the event of an incident;

[177] Unofficial translation of the LAW 125(I) of 2018 Providing for the Protection of Natural Persons with Regard totThe Processing of Personal Data and for the Free Movement of Such Data
https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/2B53605103DCE4A4C225826300362211/$file/Law%20125(I)%20of%202018%20ENG%20final.pdf, [Last accessed 31 August 2022]

[178] Office of the Commissioner for and Personal Data Protection Cyprus, "INDICATIVE LIST OF PROCESSING OPERATIONS SUBJECT TO DPIA REQUIREMENTS UNDER ARTICLE 35(4) OF THE GDPR" (n.d.), https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/ED786DE02E8020FCC225826000377143/$file/Indicative%20DPIA%20list.pdf, [Last accessed 31 August 2022].

- A **process for regularly testing, assessing and evaluating the effectiveness** of technical and organisational measures for ensuring the security of the processing;
- Special **limitation of transmission** of personal data to a third country; or
- Special **limitation of personal data processing** for some other purposes.

Moreover, the controller or processor shall further process special categories of personal data in a **form that does not permit the identification of the data subject unless this is prevented by the legitimate interests of the data subject**.

Denmark

Section 10 of the Data Protection Act of Denmark (hereafter the **Danish DPA**) regulates the processing of **special categories of data and data related to criminal offences for the purpose of scientific studies of significant importance to society**, permitting it when necessary to carry out these studies.

At the same time, section 11 (3) of the Danish DPA allows the data controller to **process the personal identification number for scientific purposes,** while section 22 (5) of the Danish DPA restricts certain data subjects' rights, specifying that Articles 15, 16, 18, and 21 of the GDPR shall not apply when the processing of data takes place exclusively for scientific purposes.

Estonia

Data protection in Estonia is primarily governed by the Personal Data Protection Act 2018 (hereafter the **Estonian PDPA**), which incorporated the GDPR into Estonia law.

Under section 6 (1) of the Estonian PDPA, the **processing of personal data is allowed for the purpose of scientific or historic research if personal data, before its transmission, is replaced by pseudonymised data or data in a format which provides an equivalent level of data protection**.

Moreover, in accordance with section 6 (2), **de-pseudonymisation or any other method by which the data enables again identification of persons** are **permitted for the needs of additional scientific and historical research**. However, in this case, the processors shall designate a single person identified by name who has access to the information allowing pseudonymisation.

Furthermore, processing of personal data for the purposes of scientific and historical research **without the consent of the data subject** in a format that enables identification of the data subject is permitted only in the case the following **conditions** are met:

1. The **purposes of data processing can no longer be achieved** after the removal of the data-enabling identification, or it would be unreasonably difficult to achieve these purposes;
2. There is an **overriding public interest** for it in the estimation of the persons conducting scientific and historical research or compiling official statistics;
3. The **scope of obligations of the data subject is not changed** based on the processed personal data, or **the rights of the data subject are not excessively damaged** in any other manner.

Finally, section 6 (4) of the Estonian PDPA specifies that if **special categories of personal data** are processed for scientific or historic research, the **ethics committee** of the area concerned shall first **verify compliance with the terms and conditions** provided in section 6. If there is no ethics committee in the scientific area, compliance with the requirements shall be verified by the **Estonian Data Protection Inspectorate.** With regard to any personal data retained at the National Archives, the **National Archives shall have the rights of the ethics committee.**

Finland

The Data Protection Act of Finland (hereafter the **Finnish DPA**) includes a number of additional safeguards based on Article 89 of the GDPR.

Section 31 (1) of the Finnish DPA specifies that the data controller, when processing personal data for the purpose of scientific research, may **derogate from Articles 15, 16, 18, and 21 GDPR**. However, in order to apply the said exception, the following **requirements** must be met:

1. The processing is based on an **adequate research plan**;
2. A **specific person or group responsible** for the research has been designated;
3. The personal data are **used and disclosed only for scientific research purposes** or for other compatible purposes, and the procedure followed is also otherwise such that data concerning a given individual are not revealed to outsiders.

Moreover, the Finnish DPA sets out several **additional requirements for processing special category data or data related to criminal offences.** In particular, whenever such data is processed for the purpose of scientific research, the data controller shall carry out a **DPIA or comply with the codes of conduct.** Finally, the data controller is required to **submit the DPIA to the Data Protection Ombudsman** before the processing.

France

Data protection in France is mainly governed by Law n° 2018-493 of 20 June 2018 and Law n° 78-17 of 6 January 1978 (hereafter the French DPA).

Based on French law, there are **no specific requirements related to general data processing for scientific or historic research purposes**. However, the French legislation imposes **stricter requirements regarding health data** processing. These requirements, set forth by the French DPA and the French Public Health Code, should be seriously considered by any company or public body, which intends to process health data for scientific research purposes. Such processing needs to additionally comply with the respective French regulations specific to medical and pharmaceutical research, as amended by a 2016 Ordinance, governing studies involving the participation of human subjects.

In view of the above, **processing of health data based on public interest requires prior authorisation from the French Data Protection Authority (hereafter CNIL),** delivered conditionally on a positive opinion of the competent committee. Nonetheless, the CNIL offers an alternative to the authorisation process. Specifically, the CNIL has published several standard methodologies, which allow the sponsor of a research project not to proceed to the authorisation process if they comply with the requirements set forth in the concerned standard methodology. In this case, the data controller before data processing must send a **declaration attesting conformity of data processing** to the CNIL.

Germany

Article 27 of the Federal Data Protection Act (hereafter the **German FDPA**) includes specific provisions regarding the **processing of sensitive data for scientific or historical research purposes**, allowing the data controller to process such data, **as long as the processing is necessary for these purposes and the data controller's interest significantly outweighs the data subject's interest**.

In order to perform the above, the data controller shall take a number of measures, including:

1. **Technical and organisational measures** to ensure that processing complies with the GDPR;

2. Measures to ensure that it is subsequently **possible to verify and establish whether and by whom personal data were input, altered, or removed**;
3. Measures to **increase awareness of staff** involved in processing operations;
4. The designation of a **DPO**;
5. **Restrictions on access** to personal data among the controller(s) and by processors;
6. The **pseudonymisation** of personal data;
7. The **encryption** of personal data;
8. Measures to ensure the **ability, confidentiality, integrity, availability, and resilience of processing systems and services** related to the processing of personal data, including the ability to rapidly restore availability and access in the event of a physical or technical incident;
9. A **process for regularly testing, assessing, and evaluating the effectiveness** of technical and organisational measures for ensuring the security of the processing;
10. Specific **rules of procedure to ensure compliance with the German FDPA and with the GDPR in the event of transfer or processing for other purposes**.

Additionally, the German FDPA requires **the anonymisation of sensitive data as soon as the research purpose allows it.** Until then, the **characteristics enabling information concerning personal or material circumstances to be attributed to an identified or identifiable individual shall be stored separately**. They may be combined with the information only to the extent required by the research or statistical purpose.

Finally, when the data controller intends to publish the personal data, he shall demonstrate that either the data subject consent for the publication or it is indispensable for the presentation of research of findings on contemporary events.

Greece

In Greece, the legal framework consists, along with the GDPR, of Law 4624/2019, implementing Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons concerning the processing of personal data, and transposition of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016, and other provisions (hereafter the **Greek DPA**) and other national implementation acts.

Under Article 30 of the Greek DPA, the **processing of special categories of personal data is permitted, without the consent of the data subject, only if it is necessary for scientific or historic research purposes** and **the data controller's interest overrides the data subject's interest**. In this respect, the data controller shall implement **appropriate and specific measures for the protection** of the data subject's interest, including **restriction of access** to the data controller and/or processor, **pseudonymisation, encryption, and the appointment of a DPO**. The special categories of personal data shall be **anonymised as soon as the research purposes allow**, unless contrary to the data subject's legitimate interest.

Finally, the data controller **may publish personal data processed in the context of the research**, as long as the data **subject has consented in writing or the publication is necessary for the presentation of the results of the research**, in which case the publication must take place only by means of pseudonymisation.

The Hellenic Data Protection Authority has provided a List of Processing Operations Subject to the Requirement of a Data Protection Impact Assessment relevant for scientific research[179].

Hungary

Act CXII of 2011 on the Right of Informational Self- Determination and on Freedom of Information (hereafter **Hungarian DPA) does not provide any specific requirements concerning the processing of personal data for scientific or historical research purposes**.

However, some **relevant provisions can be found in other sectoral regulations, such as:**

- **Act XLVII of 1997** on Processing and Protection of Medical and Other Related Personal Data (Medical Data Act);
- **Act CXIX of 1995** on the Use of Name and Address Information Serving the Purposes of Research and Direct Marketing (Hungarian Direct Marketing Act);
- **Act XXI/2008** on the Protection of Human Genetic Data (Human Genetic Info Act).

A **List of Processing Operations Subject to the Requirement of a Data Protection Impact Assessment**, relevant for data processing for scientific research purposes, can be found on the website of the Hungarian National Authority for Data Protection and Freedom of Information[180]**.**

Iceland

While Iceland is a member of the European Economic Area (hereafter EEA), it is not an EU Member State. Nonetheless, the GDPR applies in the EEA by virtue of Decision No. 154/2018 of the EEA Joint Committee. Thus, the GDPR was implemented in Iceland with Act 90/2018 on Privacy and Processing of Personal Data (hereafter the Icelandic Act).

Under Article 18 of the Icelandic Act, the **processing of data for scientific and historic research purposes in the public interest shall be subject to appropriate safeguards**, including organisational and technical measures. In case when provisions of Articles 15, 16, 18, 19, and 21 of the GDPR shall not apply, the data subject shall have the right to provide a statement to be kept with any documentation containing his or her personal data.

Ireland

Article 42 of the Irish Data Protection Act 2018 (hereafter the **Irish DPA**) incorporates the GDPR in the Irish national legal order. The Irish DPA requires data controllers, when processing personal data for scientific or historical research purposes, to take **suitable and specific measures to safeguard the fundamental rights and freedoms of the data subject and to respect the principle of data minimisation**.

Moreover, the Irish DPA specifies that if the research purpose can be fulfilled by processing, which does not permit or no longer permit the identification of the data subject, then the data controller shall process the data in that manner.

[179] Hellenic Data Protection Authority, "Data Protection Impact Assessment," n.d., https://www.dpa.gr/sites/default/files/2020-12/article_35_dpia_list_en.pdf, [Last accessed 31 August 2022].

[180] Hungarian National Authority for Data Protection and Freedom of Information, "GDPR 35 (4) Mandatory DPIA - List of Processing Operations Subject to DPIA GDPR 35 (4)," n.d., https://www.naih.hu/data-protection/gdpr-35-4-mandatory-dpia-list, [Last accessed 31 August 2022].

Italy

Legislative decree no. 196 of 30 June 2003 (hereafter the **Italian DPA**) sets up **additional rules and requirements** for processing personal data for scientific or historical research purposes.

In the first place, Article 101 of the Italian DPA **prohibits the use of personal data that has been collected for historical research purposes, for taking measures, or issuing provisions against the data subject in administrative matters**. On the contrary, this article specifies that any document containing personal data that is processed for historical research purposes may be used **only if it is relevant and indispensable for such purpose and by having regard to its nature**.

Secondly, under Article 105 of the Italian DPA, the personal data that has been collected for scientific research purposes **shall not be used for taking decisions or measures concerning the data subject or processed for different purposes**. Also, following Article 105 (2), the data controller shall **specify unambiguously the precise scientific research purpose and inform the data subject accordingly**. However, this requirement can be **overcome if it entails a disproportionate effort** with the regard to the data subject right on the condition that that information has been appropriately publicised as laid down by the rules of conduct.

Additional requirements are provided for the processing of health data according to Article 110 of the Italian DPA. Particularly, the Italian DPA requires the data controller to **conduct a DPIA and publish it** when processing the health data for scientific research in the medical, bio-medical, or epidemiological sectors, without the consent of the data subject under Article 9(2), letter j) of the GDPR, including research that is part of a biomedical or health care research programme according to Section 12-a of legislative decree No 502 of 30/12/1992.

Besides, **the consent of data subjects for processing health data is not required if informing the data subjects proves impossible or entails a disproportionate effort on specific grounds, or if it is likely to render impossible or seriously impair the achievement of the research purposes**. However, in this case, the data controller shall take **appropriate measures to protect the rights, freedom, and legitimate interest of the data subject**. Additionally, the research programme shall be the subject of a reasonable, favourable opinion by the geographically competent ethics committee as well as being submitted to the Italian Supervisory Authority for prior consultation.

Nevertheless, the data controller shall process personal data for the purposes of historical or scientific research following the rules of conduct adopted by the Italian Supervisory Authority.

Latvia

The Latvian legislation provides no deviations from the GDPR, while a list of Processing Operations Subject to the Requirement of a Data Protection Impact Assessment can be found on the website of the Data State Inspectorate of the Republic of Latvia[181].

Liechtenstein

The GDPR has been implemented into the Liechtenstein law by virtue of the Data Protection Act of 4 October 2018 (hereafter DSG) and the Data Protection Ordinance of 11 December 2018 (hereafter DSV).

[181] Data State Inspectorate of the Republic of Latvia, "List of Processing Operations Requiring Data Protection Impact Assessment Pursuant to Article 35 (4) of the GDPR," n.d., https://edpb.europa.eu/sites/default/files/decisions/lv_sa_dpia_final_list_20181212.pdf, [Last accessed 31 August 2022].

Under Article 27(1) of the DGS, the **special categories of data may be processed without the consent of the data subject for historical or scientific research purposes** if the processing is **necessary** for these purposes, and the **interest of the controller outweighs the legitimate interests of the data subject**.

In relation to the **non-special categories of personal data**, the data controller may process personal data for scientific and historical research purposes **in the public interest** if the processing is necessary for these purposes, and **if the data is publicly accessible**, or the data is **pseudonymised** and the controller cannot identify the data subject with legal measures, or **if getting the consent of the data subject is impossible or involves a disproportionate effort** due to the lack of reachability.

Moreover, the DSG requires the data controller to ensure **appropriate and specific measures to safeguard the interests of the data subject** according to Article 21(2), which shall consist of the following:

1. **Technical and organisational measures** to ensure that processing complies with the GDPR;
2. Measures to ensure that it is subsequently **possible to verify and establish whether and by whom personal data were input, altered, or removed**;
3. Measures to **increase awareness of staff** involved in processing operations;
4. The designation of a **DPO**;
5. **Restrictions on access** to personal data among the controller and by processors;
6. The **pseudonymisation** of personal data;
7. The **encryption** of personal data;
8. Measures to ensure the **ability, confidentiality, integrity, availability, and resilience of processing systems and services** related to the processing of personal data, including the ability to rapidly restore availability and access in the event of a physical or technical incident;
9. A **process for regularly testing, assessing, and evaluating the effectiveness** of technical and organisational measures for ensuring the security of the processing;
10. Specific **rules of procedure to ensure compliance with the German FDPA and with the GDPR in the event of transfer or processing for other purposes**.

In addition to the above-mentioned measures, **all personal data shall be anonymised as soon as the historical or scientific research purpose allows**. Finally, the controller may publish personal data only if the data subject provided consent or the data is indispensable for the presentation of research findings.

The conditions of necessity for a Data Protection Impact Assessment have been published on the Lichtenstein Data Protection Authority's website[182].

Lithuania

The relevant Lithuanian Act contains no provisions on the processing of personal data for scientific and historical research purposes, while a DPIA may be required under certain conditions[183].

[182] DATENSCHUTZSTELLE and FÜRSTENTUM LIECHTENSTEIN, "List of Processing Operations According to Art. 35 (4) GDPR, for Which the Data Protection Authority as the Supervisory Authority for GDPR in Liechtenstein Requires a Data Protection Impact Assessment (DPIA).," n.d., https://www.datenschutzstelle.li/application/files/7615/9670/5293/DPIA_list_Liechtenstein_EN.pdf, [Last accessed 31 August 2022].

[183] DIRECTOR OF THE STATE OF LITHUANIA -DATA PROTECTION INSPECTORATE, "ORDER ON THE APPROVAL OF THE LIST OF DATA PROCESSING OPERATIONS SUBJECT TO THE REQUIREMENT TO PERFORM DATA PROTECTION IMPACT ASSESSMENT," n.d., https://edpb.europa.eu/sites/default/files/decisions/lt-dpia_list_en_20190314.pdf, [Last accessed 31 August 2022].

Luxembourg

The GDPR has been implemented into Luxembourg Law by Act of 1 August 2018 on the Organisation of the National Commission for Data Protection and Implementing the GDPR (hereafter the Luxembourg DPA).

Under Article 65 of the Luxembourg DPA, the data controller, when processing the personal data for scientific or historical research purposes, shall implement the following measures:

1. The appointment of a **data protection officer**;
2. The performance of an **impact assessment** of the planned processing activities on the protection of personal data;
3. The **anonymisation and pseudonymisation**, or other operational separation measures guaranteeing that the data collected for scientific or historical research purposes or statistical purposes, cannot be used to adopt decisions or take actions concerning data subjects;
4. The use of a **trusted third party, operationally independent from the controller, for the anonymisation or pseudonymisation** of the data;
5. The **encryption** of personal data in transit and at rest, as well as state of the art key management;
6. The use of **technology reinforcing the protection of the private lives** of data subjects;
7. The use of **access restrictions** to personal data within the controller;
8. The use of a **log file** enabling the reason, date and time that data is consulted and the identity of the person collecting, modifying or deleting personal data to be retraced;
9. Promoting the **awareness of the** involved **staff** about the processing of personal data and professional secrecy;
10. The **regular evaluation of the effectiveness** of the technical and organisational measures implemented through an independent audit;
11. The prior drawing up of a **data management plan**;
12. The adoption of the **sector-specific codes of conduct**.

It is not mandatory for a controller to automatically implement all the measures when processing personal data for scientific or historical research purposes. However, if some measures are not implemented, the controller must document and justify each exclusion of the above-mentioned measures.

Malta

The GDPR has been implemented into Maltese law by the CAP 586 (hereafter Maltese DPA). Under Article 6 of the Maltese DPA, controllers and processors may derogate from the provisions of Articles 15, 16, 18, and 21 of the GDPR for the processing of personal data for scientific or historical research purposes under conditions that the exercise of the above-mentioned rights is likely to render impossible or **seriously impair the achievement of those purposes**, and the data controller reasonably believes that **such derogation is necessary** for fulfilment of those purposes.

Furthermore, the genetic, biometric, and health data may be processed where the research activities are **in the public interest**. However, the controller shall consult with, and obtain **prior authorisation** from, the Commissioner where the controller intends to process such data for the above-mentioned purposes. A **DPIA** may also be required[184].

[184] Information and Data Protection Commissioner for Malta, "Data Protection Impact Assessment (DPIA)," n.d.

Netherlands

In the Netherlands, the GDPR and the Dutch GDPR Implementation Act mainly govern the processing of personal data.

Under Article 44 of the Act, when the processing of personal data takes place for scientific research by institutions or services and the necessary measures have been taken to ensure that personal data can only be used for such purpose, then the controller may refrain from observing Articles 15, 16, and 18 of the GDPR.

Norway

The Norwegian Personal Data Act of 15 June 2018 (hereafter the Norwegian DPA) which implements the GDPR, does not provide variations from Article 89 of the GDPR. However, various pieces of sectoral legislation impact data protection, including the Health Research Act, Regulation on the organisation of medical and health research, and the Research Ethics Act.

The only exception as per sections 9 and 11 of the Norwegian DPA, special categories of personal data and criminal conviction data may be processed without consent for scientific or historical research purposes, provided that the benefits for the society clearly exceed the detriment to the data subject.

Poland

The Personal Data Protection Act of 10 May 2018 (hereafter the Polish DPA) entered into force on 25 May 2018 to help implement the GDPR in Poland. The Polish DPA does not introduce any legal grounds for personal data processing for historical and scientific purposes.

However, some Polish sectoral acts provide specific legal bases for various activities. For instance, the Act of 21 February 2019 Amending Sectoral Acts (hereafter the ASA) introduced changes to the sectoral laws in order to implement the GDPR requirements in the Polish legal system.

In the first place, the ASA adjusts the Act on the Higher Education (hereafter the Act) regulating data processing for scientific research purposes. The changes apply only to the entities and institutions listed in this Act. Under the Act, the processing of special category data for scientific research is permitted provided that the **publication of the results takes place in a way that prevents the identification of individuals.** Moreover, the Act requires the implementation of **specific security measures for personal data processing in relation to scientific research**. The Act, following the provisions of the GDPR, allows the exclusion of Articles 15, 16, 18, and 21 of the GDPR if it is likely that the law specified in these provisions will prevent or seriously impede research and development purposes and if the mentioned exemptions are necessary to achieve these goals.

Finally, the ASA provides changes to the Act on the Information System in Health Care, under which the data included in the medical records can be made available for the purpose of scientific research only in anonymised form.

Portugal

When the personal data are processed for scientific or historical research purposes, Article 31 of Law no. 58/2019 (hereafter Portuguese Data Protection Law) requires the data controller to include data **anonymisation or pseudonymisation** whenever such purpose can be achieved by one of these means. Moreover, the Portuguese Data Protection Law specifies that if personal data are processed for scientific research purposes, the **ethical standards** recognised by the scientific community shall be respected.

Romania

The legal rules on data protection in Romania are mainly set in Law No. 190/2018 Implementing the General Data Protection Regulation (hereafter the Romanian Data Protection Law), which **reiterates the GDPR rules and requirements concerning scientific or historical research**.

On that note, the National Supervisory Authority for Personal Data Processing (hereafter the ANSPDCP) has released guidance for the application of the GDPR[185], along with guidance on frequently asked questions on the implementation of GDPR and the applicability of Romanian Law No. 190/2018[186]

Finally, Under Decision No. 174/2018, the ANSPDCP established the activities that shall result in a high risk to the rights and freedoms of natural persons and, therefore, a DPIA is required[187].

Slovakia

There are no deviations from the GDPR in Slovakian legislation.

Slovenia

The new Slovenian Personal Data Protection Act that will implement certain aspects of the GDPR has not yet been officially adopted and is still in the legislative process. Nevertheless, the Personal Data Protection Act (hereafter the **Slovenian PDPA**) that entered into force in 2004 still applies as the principal Slovenian national legislation on personal data protection.

Article 17 of the Act allows the further processing of personal data for historical or scientific research purposes. However, the aforementioned article sets up **specific requirements** that shall be fulfilled in this case. In the first place, the personal data shall be supplied to the data recipient for further processing in the **anonymised form**, although this requirement can be exempt if otherwise provided by a relevant statute or the data subject gave prior written consent for the data to be processed without anonymising.

Furthermore, the personal data supplied to the data recipient shall be **destroyed on completion** of processing, while the data recipient is required to inform in writing the data controller after the destruction on when and how the personal data were destroyed.

Finally, the **result of processing for historical or scientific research purposes shall be published in anonymised form**, unless otherwise provided by the statute or the data subject gave written consent for publication in a non-anonymised form.

Spain

Organic Law 2/2018 on Data Protection and Guarantee of Digital Rights (hereafter the Spanish Data Protection Act) **does not provide additional requirements** or provisions concerning scientific or historical research.

[185] National Supervisory Authority For Personal Data Processing in Romania, "Guidelines for the Application of the General Data Protection Regulation by the Data Controllers," n.d.

[186] National Supervisory Authority For Personal Data Processing in Romania, "GUIDELINES Q&A WITH REFERENCE TO THE APPLICATION OF REGULATION (EU) 2016/679," n.d.

[187] National Supervisory Authority for Personal Data Processing in Romania, "Decision No. 174 of the 18th of October 2018 on the List of Kind of Processing Operations Which Are Subject to the Requirement for a Data Protection Impact Assessment," n.d.

However, in order to assist the data controllers in identifying kinds of data processing that require the Data Protection Impact Assessment, the Spanish Supervisory Authority has published "the list of the types of data processing that requires a data protection impact assessment under Article 35.4"[188]. This list sets out what kind of processing requires a DPIA and facilitates their identification for the data controllers.

Sweden

The Swedish Act containing Supplementary Provisions to the EU General Data Protection Regulation (SFS 2018:218) (hereafter the **ACSP**) **does not provide additional requirements** or provisions concerning scientific or historical research. However, a vast number of sector-specific acts have been adopted in Sweden, such as the Swedish Act concerning the Ethical Review of Research Involving Humans (hereafter the Swedish Ethical Review Act) is inter alia applicable when research involves sensitive personal data and personal data regarding criminal offences.

When a data controller processes personal data for scientific research purposes under the GDPR, there is a risk that the processing will be subject to the Ethical Review Act. If a data controller's planned research falls within the scope of the Ethical Review Act, they will have to seek **approval from the Swedish Ethical Review Authority** in relation to each research project.

Furthermore, the Ethical Review Act sets out the specific requirements which shall be fulfilled in order to conduct scientific research. In the first place, the research may only be carried out on the ground of the **data subject's consent**, which shall be **voluntary, explicit, and specific** to particular research. If the data subject is over 15 years old but has not attained the age of 18, he or she shall personally be given information about the research and consent to the research. In other cases, when the data subject has not attained the age of 18, the subject's guardians are to be informed, and their consent is to be acquired.

Also, in accordance with section 16 of the ACSP, **prior to giving the consent the data subject as to be informed** about:

- the **overall plan** for research;
- the **purpose** of the research;
- the **methods** that will be used;
- the **consequences and risks** that the research might entail;
- the identity of the **responsible research body**;
- the fact that **participation in the research is voluntary**;
- the right of the research subject to **cease participation** at any time.

However, the Ethical Review Act, under certain conditions specified in sections 21 and 22, allows the data controller to conduct the research **without the consent** of the data subject, if illness, mental disorder, a weakened state of health, or some similar circumstance prevents the subject from expressing an opinion.

Switzerland

The Federal Act on Data Protection (hereafter Swiss FADP) is the key act regulating data protection in Switzerland.

[188] Spanish Data Protection Authority, "List of the Types of Data Processing That Requires a Data Protection Impact Assessment under Article 35.4," n.d., https://www.aepd.es/sites/default/files/2019-09/listas-dpia-en-35-4.pdf, [Last accessed 31 August 2022].

In accordance with Article 22 paragraph 1 of the Swiss FADP, federal bodies may process personal data for research purposes if:

a) the data is rendered **anonymous**, as soon as the purpose of the processing permits;
b) the recipient only discloses the data with the **consent of the federal body;** and
c) the **results are published in such a manner that the data subjects may not be identified.**

Additionally, under Article 4 paragraph 3 of the Swiss FADP the personal data may only **be processed for the purpose indicated at the time of collection, that is evident from the circumstances, or that is provided for by law**. Furthermore, Article 17 paragraph 2 specifies that the personal data may be processed by federal bodies only if a formal enactment expressly provides therefor. However, such data may also be processed, by way of **exception** when:

a. such processing is **essential for a task clearly defined** in a formal enactment;
b. the **Federal Council authorises processing in an individual case** because the rights of the data subject are not endangered; or
c. the **data subject has given his consent** in an individual case **or made their data general accessible** and has not expressly prohibited its processing.

Finally, following the article 19 paragraph 1 of the Swiss FADP federal bodies may disclose personal data if there is a legal basis for doing so in accordance with Article 17 or if:

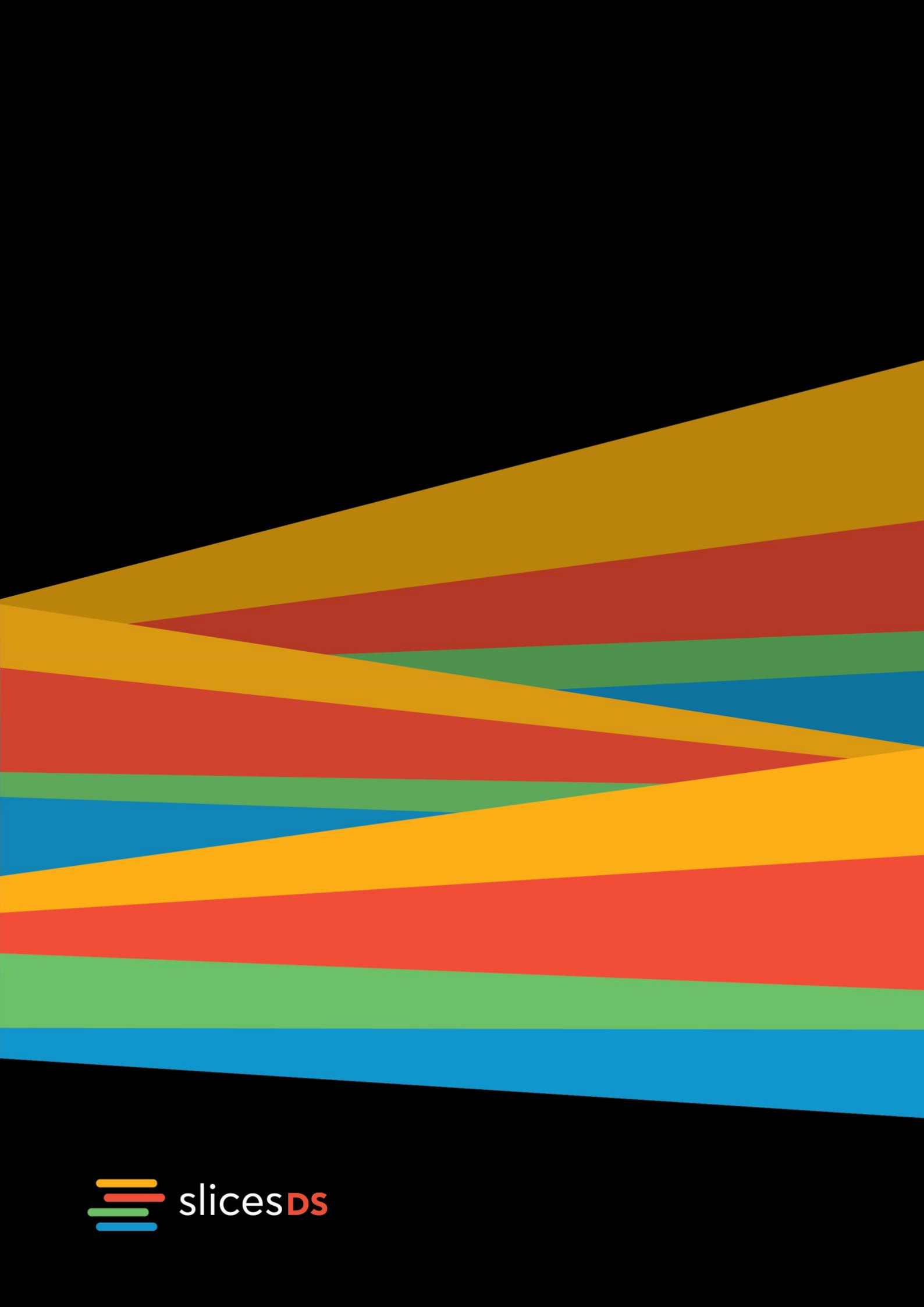
i. the data is **indispensable to the recipient** in the individual case for the fulfilment of their statutory task; or
ii. the data subject has **consented** in the individual case; or
iii. the data subject has **made the data generally accessible and has not expressly prohibited disclosure**; or
iv. the recipient demonstrates credibly that **the data subject is withholding consent or blocking disclosure in order to prevent the enforcement of legal claims or the safeguarding of other legitimate interests**. In this case, the data subject must if possible be given the opportunity to comment beforehand.

United Kingdom

In the United Kingdom, the key pieces of legislation governing data protection are the UK General Data Protection Regulation (hereafter the **UK GDPR**) and the Data Protection Act (the UK DPA).

In accordance with Article 89 of the UK GDPR the data controller in order to process personal data for scientific or historic research purposes must adopt **appropriate safeguards** to protect data subjects, and in particular technological and organisational measures to ensure data minimisation. Those measures may include **pseudonymisation**.

Section 19 of the UK DPA contains further safeguards. In particular, the data controller must be able to demonstrate that the processing of personal data for scientific or historic research **is not likely to cause the substantial damage or distress to the data subject** and **the data controller must not use the data to take any action or make decisions in relation to the data subject** unless the purposes for which the processing is necessary to include the purposes of approved medical research.


slicesDS