Ref. Ares(2024)5170372 - 16/07/2024

HORIZON 2020
H2020 - INFRAIA-2020-1

# D7.2 ELES Report

| | |
|---|---|
| Acronym | SLICES-SC |
| Project Title | Scientific Large-scale Infrastructure for Computing/Communication Experimental Studies – Scientific Community |
| Grant Agreement | 101008468 |
| Project Duration | 42 Months (01/03/2021 – 31/08/2024) |
| Due Date | 30 June 2024 (M40) |
| Submission Date | 16 July 2024 (M41) |
| Authors | Adrian Quesada Rodriguez, Vasiliki Tsiompanidou, Lisa Sieker, Maria Roglekova, Dolina Tziotzora, Iida Lehto, Renata Radocz, Sébastien Ziegler, Ana María Pacheco (MI) |
| Reviewers | Anna Brékine (IoTLAB), Brecht Vermeulen (IMEC) |

*This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101008468. The information, documentation and figures available in this deliverable, is written by the SLICES-SC 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.*

Scientific Large-scale Infrastructure for Computing Communication Experimental Studies **Starting Communities**

www.slices-sc.eu

## Executive summary

The aim of this report is to consider and analyse the legal and ethical context that should govern the entire project, as well as to identify the potential economic and social aspects of the SLICES-SC project.

More precisely, the SLICES project seeks to design and implement a Europe-wide test-platform, to support large-scale, experimental research focused on networking protocols, radio technologies, services, data collection, parallel and distributed computing and in particular cloud and edge-based computing architectures and services. The SLICES-SC (Scientific Community) project, more precisely, aims at designing and deploying the necessary solutions that will enable its adoption by users. In order to achieve this, SLICES-SC is building and expanding a community of researchers that will benefit from the infrastructure. As such, a concrete focus is placed on ensuring access to these research experiments, their reproducibility, and the validation and publication of the results.

Taking the above parameters into consideration, the present deliverable focuses on two primary aspects of the SLICES-SC project: the compliance approach for the relevant ethical and legal framework, and building upon these elements, and on relevant socio-economic considerations to develop relevant guidance for future developments of the SLICES-RI, particularly as necessary to meet applicable administrative and due-diligence requirements. In order to identify the potential challenges that the project may be called to face, the present deliverable presents and analyses relevant legislation and requirements at both an international and a European level, as well as the relevant applicable international data transfer standards. Based on the above, the deliverable provides a series of baseline guidance that partners of SLICES-SC project can utilise to design and implement their activities in a manner that is compliant with relevant legislation and promotes data reuse and ethics. These guidelines aim to cover all stages of the project's lifecycle and include provisions on how to share data within and beyond the Consortium in order to foster data reuse beyond the project's lifetime and constantly promote and expand research in the field of innovation and cutting-edge technologies. Given the nature and processes associated with ethical and legal compliance assessment and data governance, the information presented in this document is expected to evolve during the project's lifetime.

Overall, strong collaboration with WP3 is foreseen as technical and operational requirements for data regulation compliance will be derived from the analysis and fed to the design of the architecture. Additionally, the report seeks to provide guidance on the legal framework of cooperation between researchers, operators, national agencies and regulatory bodies.

## Table of Contents

## List of Figures

# 1. Introduction

As the SLICES Research Infrastructure (SLICES-RI) seeks to generate a Europe-wide digital test-platform to support large-scale, experimental research that will provide advanced computation, storage and network components, interconnected by dedicated high-speed links, SLICES-SC aspires to foster the community of researchers around this ecosystem, as well as create and strengthen necessary links with relevant industrial stakeholders for the eventual exploitation of the infrastructure. As such, it is clear that SLICES seeks to have a positive social impact and play a significant role on the amelioration of the EU economy and stimulating innovation.

More specifically, the SLICES-SC (Scientific Community) projects' main key objectives are the following:

- The creation of a network of researchers for knowledge sharing and collaboration on projects;
- The creation and strengthening of links with relevant industrial stakeholders for the exploitation of the infrastructure;
- The advancement of existing methods for research reproducibility and experiment repeatability;
- The creation of infrastructure for wider audience;
- The design and deployment of innovative solutions for providing SLICES-RI with an easy to access scheme for users from different disciplines.

In the context of the SLICES-SC project, compliance with ethical and legal considerations as well as with environmental, economic and societal values has not only been ensured and upheld, but seeks to develop sufficient information on how the SLICES-RI should continue to address such considerations. This deliverable seeks to clarify a way forward for SLICES to comply with an increasingly complex regulatory and ethical framework, while bolstering economic and socially impactful research.

## 1.1 Methodology

This Deliverable identifies and presents an analytical overview of the Ethic, Legal, Economic, and Social aspects addressed by the SLICES-SC project and provides relevant information and guidance for the SLICES-RI. Given its nature as a large-scale project, SLICES-SC requires a carefully designed and systematically coordinated approach to ensure legal and ethical compliance amongst its various stakeholders. More specifically, this document focuses on overviewing the regulatory frameworks, including the applicable legislations and relevant sources of ethical principles and requirements in Europe, while in its analysis it gives a special emphasis on the cross-border data transfer standards in the context of research and experimentation. The development of cutting-edge technologies and the creation of technological and experimental resources requires that data governance must be responsible, encompassing legal, ethical and social requirements. Therefore, the present deliverable focuses on the ways the development of technologies can be designed ethically while still fostering data protection and innovation. To that end, it identifies the respective ethical risks and requirements, to ultimately provide guidance on ethical data governance, data-sharing policy and compliance with regulatory frameworks.

This report further carries out a comparative analysis of relevant regulations and standards, by providing a meticulous legal framework and international standards mapping (see Annex 1: Legal framework mapping to SLICESand Annex 2: Mapping with relevant standards), and it identifies the necessary administrative and compliance procedures that should be considered in the context of the project's specific activities. In the pertinent section, this deliverable attempts to tailor the legal and ethical considerations to the unique demands of varying countries. By addressing the country-specific

ethical requirements, SLICES-SC can ensure the responsible use of its infrastructure, promoting innovation in a compliant manner. Furthermore, as SLICES-RI intends to address a large and diverse community of users and researchers regarding geographical location, background and industrial involvement, and thus, bring about a large societal impact, this report delves into a thorough analysis of the economic and social effects and implications that this project can present. More precisely, this report examines and highlights the social aspects and benefits that SLICES-RI will bring to the table for consumers and citizens in general. Concerning the effect of the project on the market, this report also examines and focuses on the specific consequences and advantages that it will generate, since through the enlargement/enhancement of research infrastructures, new employment opportunities will be created, which will, in turn, economically have a significant impact on the market.

Leveraging on all the theoretical framework, this deliverable aims to assist SLICES-SC and SLICES-RI partners to better perform upcoming activities and administrative tasks in a way that is compliant with both legal and ethical requirements. The deliverable also examines relevant socio-economic considerations that should be considered for future developments. Furthermore, it leverages on the identified fundamental principles that guide the project to present a comprehensive layer of information regarding the project's legal and ethical compliance activities.

### 1.2 SLICES-RI – Brief introduction

SLICES-RI is intended to connect the community of researchers, develop and provide services 'related to experimentation in the context of digital sciences such as 5G, 6G, Network Functions Virtualization (NFV), Internet of Things (IoT) and cloud computing'. In order to achieve this, SLICES-RI focuses on establishing a pan-European, distributed Research Infrastructure that enables research across countries and industries to perform large-scale innovation activities.

In this context, the SLICES-SC project aims at designing and deploying the necessary solutions that will enable its adoption by users. Thus, SLICES-SC is building and expanding a community of researchers that will benefit from the infrastructure. As such, a concrete focus is placed on ensuring access to these research experiments, their reproducibility, and the validation and publication of the results.

As a 'Europe-wide test-platform, to support large-scale, experimental research', SLICES is a project of relevance to multiple stakeholders, which will join its community (SLICES-SC), by generating a network to link research infrastructures, with actors that could benefit from it, such as academia, industry and business actors in a long-term and sustainable way.

This being considered, the SLICES governance framework was planned as having 'a centralized governance and a central hub'. As such, this central hub is composed of the Coordination and Management Office and the Support team including supporting professionals. The decision-making body is the Supervisory Board (SB), which is composed of one academic and one ministry/financing agency representative per country. At its current stage, however, the main decision-making body for SLICES-RI is the Interim Supervisory Board (ISB), which 'aims to work pro-actively and constructively to set up SLICES-RI as a sustainable European Research Infrastructure Consortium'.

In order to emphasize the dedication to the needs of its users, which is, by definition, required for a research infrastructure according to relevant requirements and guidance from the European Commission, the SLICES governance includes a dedicated Users Committee for several of the connected projects, such as SLICES-SC.

As such, it is of relevance to clarify that SLICES targets 4 different kinds of users, which will be granted access to the state-of-the-art infrastructure and tools for deploying innovative experiments. These include (1) the Research User Group including, for example, academia, (2) the Industry User Group

focusing on business-oriented organisations, (3) the Research/Industry Support User Group and (4) the External Partners User Group including, for example, compliance officers. This is of relevance to this Deliverable, as it enables a better understanding of the types of actors interested in the infrastructure and the potential areas of research which could be carried out in the SLICES infrastructure.

## 2 Ethical considerations

This section focuses on the analysis of the ethical considerations and requirements that are particularly applicable in the fields of science, technology, and artificial intelligence, considering their importance for the SLICES-SC project. In the past years, ethics has evolved into a crucial element for research, not solely as a compliance measure but also as a fundamental responsibility toward stakeholders, users, and society as a whole. As such, ethics has been subject to a systematic effort of codification, with regulators embedding ethics into standards, normative sources and legislation, ensuring that innovation is aligned with human rights and societal values.

In addition to the above, the integration of ethical principles in the development and use of AI and advanced technologies is vital for fostering public trust and acceptance, enabling the rapid expansion of the infrastructure. Ethical principles including data privacy, security, and the prevention of biases in AI algorithms, while addressing potential environmental impacts play a major role in fostering trust with the users of the infrastructure.

As SLICES-SC engages with a diverse user community, establishing robust guidelines for the responsible and ethical use of its infrastructure is essential. The ethical requirements analysed below promote an environment of integrity, transparency, and fairness and guide the use of the SLICES infrastructure. As such, SLICES-SC strives to maintain the highest standards of integrity, responsibility, and societal benefit in advancing large-scale digital sciences.

By incorporating these ethical dimensions from the project's design phase, SLICES-SC not only enhances its research outcomes but also contributes positively to the broader societal discourse on the role of technology in human life. Consequently, by embedding ethical considerations at the core of its operations, SLICES-SC aims to lead by example in promoting responsible innovation. This commitment helps safeguard against ethical lapses, supports the fair distribution of technological benefits, and ultimately advances the public good in the digital age.

### 2.1 Relevant sources of ethical requirements

As already highlighted above, in the rapidly evolving landscape of technology and scientific innovation, ethical considerations play an increasingly central role in shaping the responsible development and implementation of cutting-edge technologies. The present section will delve deeper into the primary ethical requirements on an international and European level and will highlight the most relevant considerations for the SLICES-SC project.

Since the SLICES-SC project is closely linked to the use of advanced technologies for research purposes, Open Science and the establishment of a community of users are of utmost importance. As a result, the normative requirements, standards, and soft law documents considered for the ethical framework represent the global acquis addressing those specific needs and guiding activities within SLICES. Drawing from a wide range of frameworks, the following subsections discuss, in particular, the ethical frameworks provided by European and International normative instruments.

***The European Code of Conduct for Research Integrity***

The All-European Academies (ALLEA) European Code of Conduct (ALLEA - All European Academies, 2023) adopts a principle-based approach to research, laying down the baseline for ethical research practices across disciplines, both public and private. It particularly defines four main ethical principles, namely:

a) Reliability, ensuring that the quality of the research methodology and the associated analysis are consistent,
b) Honesty, providing for transparency and fairness throughout the entire research process,
c) Respect, regarding the behaviour of the researchers towards the other researchers/different groups
d) Accountability, defining the behaviour of the organization that is conducting the research and the wider societal impacts that this behaviour may have.

Said research principles are applicable in all research contexts, including, in particular:

- the Research Environment;
- Training, Supervision, and Mentoring;
- Research Procedures;
- Safeguards;
- Data Practices and Management;
- Collaborative Working;
- Publication, Dissemination, and Authorship;
- Reviewing and Assessment.

Figure 1 below presents an in-depth analysis of good research practices, categorized by context, that stem from the above principles, as presented in the 2023 edition of the European Code of Conduct for Research Integrity.

| Context | Reliability | Honesty | Respect | Accountability |
|---|---|---|---|---|
| Research Environment | Research organisations should ensure a culture of research integrity by promoting awareness | Research organisations should have clear, transparent and fair research policies | Research organisations should create an environment of mutual respect | Research institutions should handle cases of misconduct and violations of research integrity |
| Research Procedures | State-of-the-art must always considered | All research processes must be documented for transparency | Be respectful of differences in research participants in the research protocol | Be accountable for properly using research funds |
| Data Management | Ensure appropriate data stewardship for clearly stated time periods | Ensure that access to data is as open as possible | Ensure transparency in how data can be accessed and used | Be compliant with GDPR |
| Publications and dissemination of Research | Authors disclose any conflict of interest and any sources of support for the publication | Authors should include author contribution statement in their publication | Authors formally agree on the sequence of authorship based on contribution | Authors and publishers promptly issue publication corrections if necessary |
| Supervisions and Trainings | Researchers should receive trainings in research design and methodology | Trainings in ethics and research integrity should be available | Senior researchers should mentor their teams and lead by example in attending trainings | Researchers should be accountable for being trained according to their career level |

Figure 1. Good research practices based on the core principles considered.

The Code additionally provides guidelines to identify any misconduct and ethically unacceptable practices that may surface. It classifies research misconduct into 3 categories, namely fabrication

(making up results), falsification (manipulating research tools or materials) and plagiarism (using others' work or ideas without giving credit). In addition, to the 3 categories, it identifies certain unacceptable practices that may not exactly fall under these categories, but should still be addressed, specifically, allowing influence by funders, misusing seniority, negatively impacting the work of other researchers, e.g. by delaying it, citing inaccurately, re-publishing work, etc. Research Integrity and the identified four aforementioned core principles are fundamental to the commitment of SLICES-SC to maintain a trustworthy scientific process and context, while ensuring that no fabrication, falsification or plagiarism of research materials and data takes place.

UNESCO Recommendation on Open Science (2021)

Open Science forms an integral part of research, ensuring that results, knowledge, and outcomes are made available to benefit the research community and society as a whole. The rationale behind this lies in the fact that the dissemination of knowledge helps foster innovation and ensure a wide adoption of technological and scientific findings. In this regard, open science is fully aligned with the Universal Declaration of Human Rights (Article 27) promoting the right to share scientific advancements and their benefits.

In the spirit of promoting open science, the UNESCO Recommendation encompasses open engagement of societal actors, open dialogue with other knowledge systems, open scientific knowledge (including publications, resources, software, hardware and research data), as well as open science infrastructures. As per the Recommendation, the core values enshrined in the entire lifecycle of research include:

a) *Quality and integrity, focusing on academic freedom, human rights and high-quality research encompassing knowledge from multiple sources made available for scrutiny;*
b) *Collective benefit, requiring that knowledge be universally shared;*
c) *Equity and fairness;*
d) *Diversity and inclusiveness.*

It has also provided for the following open science principles:

a) *Transparency, scrutiny, critique and reproducibility;*
b) *Equality of opportunities;*
c) *Responsibility, respect and accountability;*
d) *Collaboration, participation and inclusion;*
e) *Flexibility;*
f) *Sustainability.*

SLICES, as a major research infrastructure, is fully aligned with the open science principle, offering a unique space for innovation and collaborative research, having introduced the above values and principles throughout the lifecycle of its activities.

UNESCO Recommendation on Ethics of Artificial Intelligence (2021)

The Recommendation sets the groundwork for ethical AI development, forming the first standard in the field and, as such, it is treated as the basis of AI ethics. The Recommendation is divided into four main sections, namely:

1. Values:

   a. respect, protection and promotion of human dignity, human rights and fundamental freedoms;
   b. environment and ecosystems flourishing;
   c. ensuring diversity and inclusiveness;
   d. living in harmony and peace.

2. Principles:
   a. proportionality and avoidance of harm,
   b. safety and security,
   c. fairness and non-discrimination,
   d. sustainability,
   e. privacy,
   f. human oversight and determination,
   g. transparency and explainability,
   h. responsibility and accountability,
   i. awareness and literacy,
   j. multi-stakeholder and adaptive governance and collaboration.
      i. Areas of Policy *action to guide organizational policies regarding AI, including Ethical impact assessments, Ethical Governance and Stewardship, Data policy, Development and international cooperation, Environment and ecosystems, Gender, Culture, Education and research, Economy and Labour, Health and social well-being.*
      ii. Monitoring and evaluation, *ensuring transparent mechanisms to evaluate existing policies.*

Ethics Guidelines for Trustworthy Artificial Intelligence by the High-Level Expert Group on AI (2019)

The High-level Expert Group on Artificial Intelligence of the European Commission had established the framework for trustworthy AI that has formed the baseline for all EU-based legislative and normative initiatives. The guidelines focus on three main elements of AI, requiring that it is:

I. lawful, complying with all applicable laws and regulations;
*II.* ethical, ensuring adherence to ethical principles and values; and
*III.* robust, both from a technical and social perspective.

Figure 2 summarises the further guidelines provided per requirement:

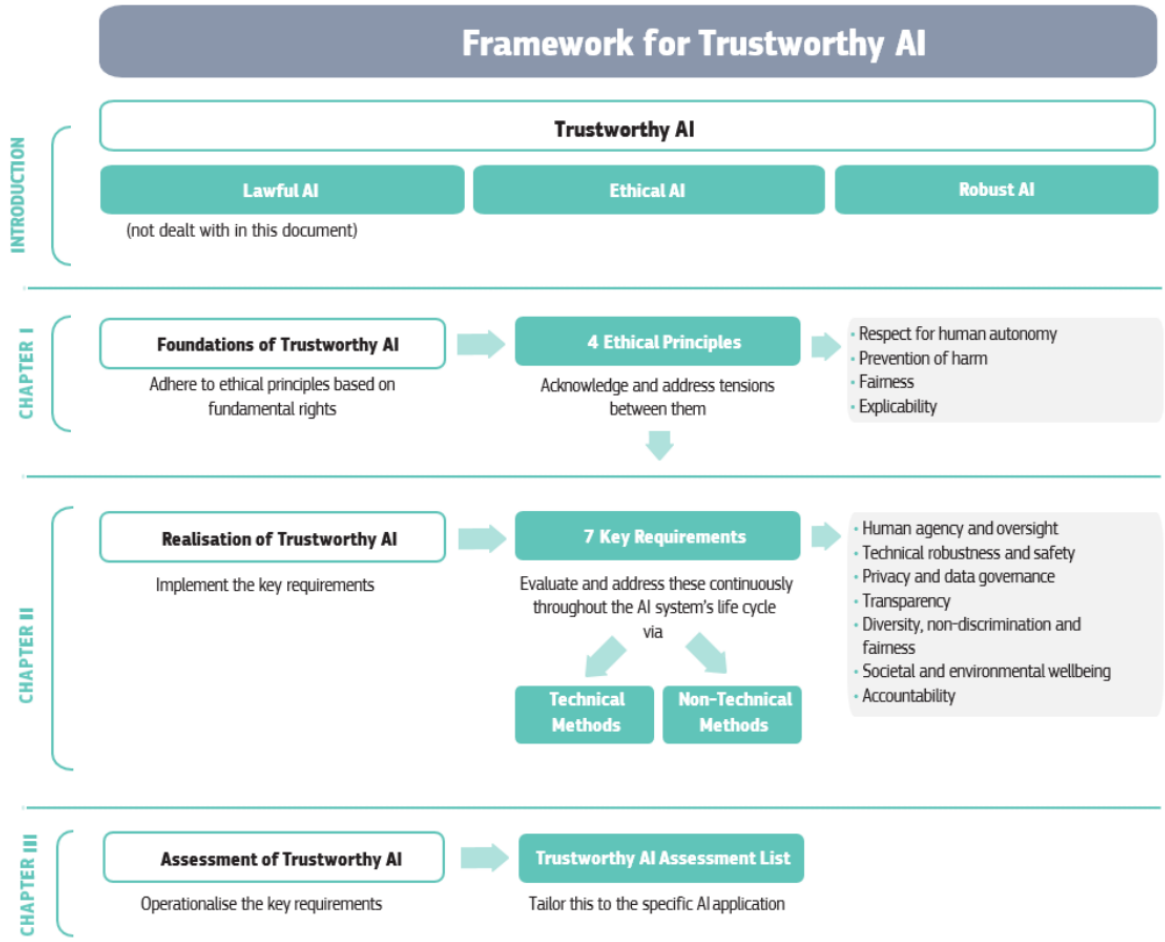



Figure 2. Guidelines as a framework for Trustworthy AI, Ethics Guidelines for Trustworthy Artificial Intelligence by the High-Level Expert Group on AI.

IEEE Ethically Aligned Design Principles – A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems (2017): IEEE Code of Ethics

The IEEE Ethically Aligned Design provides for the following general principles meant to lead the design, development and implementation of intelligent and autonomous technologies:

*a.* Human Rights, ensuring that the technologies do not infringe on internationally recognized human rights;
*b.* Well-being, prioritizing relevant metrics in their design and use
*c.* Accountability, ensuring assumption of responsibility;
*d.* Transparency;
*e.* Awareness of misuse, minimizing relevant risks.

OECD Principles for trustworthy AI (2019)

The OECD has developed the following principles for responsible stewardship of trustworthy AI to be considered by all actors involved in the development and implementation of AI systems:

a. Inclusive growth, sustainable development and well-being;

*b.* Respect for the rule of law, human rights and democratic values, including fairness and privacy;
*c.* Transparency and explainability;
*d.* Robustness, security and safety;
*e.* Accountability.

The above principles were further re-instated in the OECD paper on AI, Data Governance and Privacy published in June 2024, highlighting their lasting importance for stakeholders involved in the development, deployment and testing of AI systems and algorithms.

### 2.2 Relevant standards

Following the abovementioned effort to codify ethics, a number of international standards have been developed encompassing ethical principles and requirements, with the goal to ease the operationalization of such requirements. Said standards include both sector-specific and technology-specific requirements, as summarised below.

ISO/IEC TR 24368:2022 - Information technology — Artificial intelligence — Overview of ethical and societal concerns

The focal point of this technical report is the provision of principles, processes and methods to address ethical and societal concerns regarding the use of AI. It comprises an overview of International Standards in the field, including ISO/IEC 24029-2: Artificial Intelligence (AI) -- Assessment of the robustness of neural networks -- Part 2: Formal methods methodology and ISO/IEC 23894 -- Information technology -- Artificial intelligence -- Risk management.

Based on these, the report has identified and provides additional information on the following key themes and principles:

- *Accountability*
- *Fairness and non-discrimination*
- *Transparency and explainability*
- *Professional responsibility*
- *Promotion of human values*
- *Privacy*
- *Safety and security*
- *Human control of technology*
- *Community involvement and development*
- *Human-centred design*
- *Respect for the rule of law*
- *Respect for international norms of behaviour*
- *Environmental sustainability*
- *Labour practices*

ISO/IEC 2600 – Social responsibility

The ISO 26000 standard provides guidance on:

- *Recognizing social responsibility and engaging stakeholders*
- *Ways to integrate socially responsible behaviour into the organization*

The seven key underlying principles of social responsibility:

- *Accountability*
- *Transparency*
- *Ethical behaviour*
- *Respect for stakeholder interests*
- *Respect for the rule of law*
- *Respect for international norms of behaviour*
- *Respect for human rights*

The seven core subjects and issues pertaining to social responsibility within the context of this standard are:

- *Organizational governance*, providing for the need for accountability, transparency, ethics, and stakeholder engagement in the organization's decision-making process
- *Human rights*, with a particular focus on:
    - *Due diligence*
    - *Human rights risk situations*
    - *Avoidance of complicity*
    - *Resolving grievances*
    - *Discrimination and vulnerable groups*
    - *Civil and political rights*
    - *Economic, social, and cultural rights*
    - *Fundamental principles and rights at work*

- *Labor practices*
- *The environment*
- *Fair operating practices*
- *Consumer issues*
- *Community involvement and development*

ISO/IEC 27701: 2019 Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines

ISO/IEC 27701 is a data privacy extension to ISO 27001. It assists organizations in establishing systems to support compliance with the European Union General Data Protection Regulation (GDPR) and other global data privacy requirements (although it is not a valid GDPR certification mechanism). This standard allows an organization to regularly review and validate the compliance status, managing any risks that may arise. As a result, it promotes the continual improvement of the system in order to ensure privacy and confidentiality protection, while addressing any vulnerabilities.

## 2.3 Country-specific ethical requirements

Given the distributed approach of the SLICES infrastructure, compliance with ethical and regulatory requirements must necessarily consider the need to address local administrative and regulatory dispositions. The following sections showcase the main requirements, sources by authorities, as well as other guidance sources that should be considered (or contacted, in the case of authorities) by SLICES-RI partners in the future.

***Belgium***

The main legislation that governs data protection in Belgium is the Act of July 30, 2018[1], which focuses on safeguarding the rights of individuals in relation to the handling of their personal data. It regulates the management of personal information by enterprises that handle or process data, irrespective of the geographical location of the processing.

The Act includes essential elements of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679), allowing Member States to enforce further standards or restrictions. The Act and the GDPR together provide the essential framework of data protection law in Belgium. Furthermore, the Act incorporates the criteria outlined in Directive (EU) 2016/680, often referred to as the Data Protection Directive for Law Enforcement. This directive governs the use of personal data by law enforcement entities and establishes the Police Information Supervisory Body.

The Belgian Data Protection Authority (DPA), also known as Gegevensbeschermingsautoriteit (GBA) in Dutch and Autorité de Protection des Données (APD) in French, is the main governing agency responsible for enforcing data privacy legislation in Belgium. The DPA offers a variety of materials for both professionals and the general public, including:

- Guidance on DPIA
  *(Available in French https://www.autoriteprotectiondonnees.be/publications/guide-analyse-d-impact-relative-a-la-protection-des-donnees.pdf )*
- Portal for Guidance on DPOs (available in French
  https://www.autoriteprotectiondonnees.be/professionnel/rgpd-/deleque-a-la-protection-des-donnees)
- Guidance on International Data Transfers: Available in French
  (https://www.autoriteprotectiondonnees.be/professionnel/themes/flux-internationaux-de-donnees ).

In Belgium, ethical compliance in research is ensured through the operation of several authorities and committees. These bodies assess research proposals, provide guidance, and guarantee the welfare of research participants. These are the following:

The **Federal Public Service** (FPS) Health, Food Chain Safety, and Environment is responsible for supervising issues pertaining to health, food safety, and the environment. The Federal Public Service (FPS) Economy, SMEs, Self-Employed, and Energy is tasked with upholding ethical standards in

[1] The whole text of the Act may be accessed at the following link (https://www.dataprotectionauthority.be/publications/act-of-30-july-2018.pdf).

economic and commercial research. Each of these bodies has a vital role in supervising and certifying ethics committees across Belgium, ensuring adherence to both national and European standards.

There are also **Local Ethics Committees** (LECs) that have the responsibility of reviewing and enforcing ethical standards in local research and testing. More specifically, each hospital, institution, and research organization in Belgium have its own unique Local Ethics Committee (LEC). These committees are mainly tasked with the job of:

- Assessing the merit of research concepts;
- Assessing the ratios of probable risks and rewards;
- Ensuring the adoption of suitable procedures to get informed consent;
- Overseeing ongoing research to ensure compliance with ethical guidelines.

Moreover, the **Belgian Ethics Committees** (ECs) have the main goal of safeguarding the safety, dignity, rights, and privacy of persons involved in clinical research, with the aim of ensuring their protection and well-being. This is carried out in accordance with Belgian law and global norms. The Ethics Committees (ECs) evaluate the scientific and ethical rigor of studies, the competence of researchers, the well-being of participants, and the voluntary nature of their involvement.

The ECs also take into account recommendations from the Belgian Advisory Committee on Bioethics and the National Council of the Order of Physicians. The Belgian Association of Research Ethics Committees (BAREC)[2] was created by Belgian ECs in June 2016 with the aim of fostering cooperation and optimizing ethical review processes.

***Cyprus***

The data protection framework in Cyprus is primarily regulated by the General Data Protection Regulation (GDPR), which was incorporated into national legislation with Law 125(I) of 2018. This law, known as the General Data Protection Regulation (GDPR), superseded the earlier Data Protection Directive and set specific criteria that are monitored by the Office of the Commissioner for Personal Data Protection. The Commissioner adopted a range of guidelines issued by the European Data Protection Board (EDPB) that pertain to topics including data protection officers, Data Protection Impact Assessments (DPIAs), notifications of personal data breaches, codes of conduct, certification mechanisms, and security protocols for data processing. These measures guarantee that personal data is managed in accordance with GDPR regulations, fostering openness and accountability in data management. More specifically, the Guidelines from the Commissioner encompass in particular:

- Data protection officers ('DPO Guidance') (*https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page2b_en/page2b_en?opendocument*)
- Data Protection Impact Assessments ('DPIA Guidance') (*https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page2c_en/page2c_en?opendocument*)
- Codes of conduct (only available in Greek *https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page2d_gr/page2d_gr?opendocument*) and certification mechanisms (only available in Greek

[2] Additional details on BAREC may be found at https://barec.be/

https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page2i_gr/page2i_gr?opendocument)

- Security of processing (only available in Greek https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page2e_gr/page2e_gr?opendocument) and the guidelines on the security of processing (available only in Greek https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/all/9B2485E1D6829E8FC225820A003F5E7C/$file/Οδηγίες%20πολιτικής%20ασφαλείας.pdf?openelement);
- Data transfers (only available in Greek https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page2f_gr/page2f_gr?opendocument);
- Guide to records of processing activities https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page2d_en/page2d_en?opendocument and Guide to complete the record of processing activities https://www.dataguidance.com/sites/default/files/guide_-_record_of_activities_eng.pdf

Regarding the ethical oversight of research, Cyprus has formed the National Bioethics Committee (NBC) under Law 150(I)/2001 to oversee ethical aspects of research. The NBC functions as the primary governing body that evaluates research proposals involving human subjects, guaranteeing compliance with ethical standards and protecting the well-being of participants. The Cyprus National Committee for Clinical Trials (CNCCT) complements the NBC by supervising the ethical and regulatory components of clinical trials, in compliance with EU standards and national legislation. Furthermore, Local Ethics Committees (LECs) at hospitals, colleges, and research institutes have a vital function in assessing and overseeing research undertakings carried out inside their particular organizations. These organizations together maintain strict ethical guidelines for research across Cyprus, creating a favourable climate for scientific honesty and the safeguarding of participants.

***Finland***

Finland is subject to the EU data protection regulations, namely the General Data Protection Regulation (Regulation (EU) 2016/679). In Finland, the GDPR and its implementation at the national level are further clarified and enhanced by the Data Protection Act (1050/2018). The Data Protection Act entered into force on January 1, 2019. According to this Act, Finnish laws regulate the handling of personal data if the controller's business is based in Finland and the processing is done as part of the activities of a controller or processor in the EU. The Data Protection Act includes provisions for the nomination, organization, and powers of the supervisory authority responsible for data protection issues. It is important to mention that the Data Protection Act states that it shall be applicable in conjunction with the GDPR. In addition, Finland has implemented particular laws and precise responsibilities for data protection and data processing on particular subjects.

One notable legislation is the Act on Electronic Communications Services, previously known as the Information Society Code (917/2014). This law, referred to as the Act 917/2014, contains regulations on the privacy of electronic communications. Act 917/2014 establishes requirements for the handling of communications data, data storage, and electronic direct marketing. The full text of the Act may be found at this link: https://www.finlex.fi/fi/laki/kaannokset/2014/en20140917_20201207.pdf.

The Office of the Data Protection Ombudsman (Tietosuojavaltuutetun toimisto) is the local supervisory authority in Finland responsible for overseeing the enforcement of data protection laws. It, along with the Deputy Data Protection Ombudsmen, ensures compliance with the General Data Protection Regulation (GDPR) and the Finnish Data Protection Act.

The Office of the Data Protection Ombudsman has also released a list called the DPIA List. This list includes processing operations that require a Data Protection Impact Assessment (DPIA), as mandated by Article 35(4) of the General Data Protection Regulation (GDPR). The DPIA List can be accessed at https://tietosuoja.fi/en/list-of-processing-operations-which-require-dpia. The DPIA List is derived from the Working Party 29 DPIA Guidelines, which provide guidance on conducting Data Protection Impact Assessments (DPIAs) and determining whether processing activities are likely to pose a significant risk as defined by Regulation 2016/679. They are available at: https://www.dataguidance.com/sites/default/files/wp29-gdpr-dpia-guidance_final.pdf. The DPIA List serves as a supplement to these recommendations and provides more specific information. It is, however, not a comprehensive list.

The Ombudsman has furthermore released the subsequent guidelines pertaining to Data Protection Impact Assessments (DPIAs):

- Guidelines on risk assessment and data protection planning; (*https://tietosuoja.fi/en/risk-assessment-and-data-protection-planning*)
- Guidelines on DPIAs (*https://tietosuoja.fi/en/impact-assessments*)
- Guidelines on prior consultation (*https://tietosuoja.fi/en/prior-consultation*) ;
- Guidance on carrying out a DPIA ('the DPIA Guidance'); (*https://tietosuoja.fi/en/carrying-out-an-impact-assessment*)

Furthermore, the European Data Protection Board (EDPB) has published the following Opinion for Finland Opinion 8/2018 on the draft list of the competent supervisory authority of Finland regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR) (25 September 2018)( https://www.edpb.europa.eu/sites/default/files/files/file1/2018-09-25-opinion_2018_art._64_fi_sas_dpia_list_en.pdf)

In addition, there exists an Expert Committee that offers statements and guidance on important inquiries and matters concerning data processing issues when requested by the Data Protection Ombudsman. At the same time, the national expert bodies responsible for assessing ethics compliance in research operations in Finland include the following:

- The Finnish National Board for Research Integrity, often known as TENK
- The National Advisory Board on Social Welfare and Health Care Ethics, ETENE (www.etene.fi/en),
- The board for Gene Technology (www.geenitekniikanlautakunta.fi/en)
- The Advisory Board on Biotechnology (www.btnk.fi/en)
- The National Committee on Medical Research Ethics – TUKIJA (www.tukija.fi/en)
- and other relevant organizations and actors are responsible for overseeing the compliance of research projects with the applicable ethical principles.

Additional pertinent organizations include:

- The Committee for Public Information in Finland
- The Federation of Finnish Learned Societies
- The Finnish Information Centre for Register Research (ReTki)
- The Finnish Social Science Data Archive
- The Ministry of Education and Culture
- The Office of the Data Protection Ombudsman
- Research ethics at the University of Helsinki

***France***

In France, the French Act No. 2018-493 of 20 June 2018 (available in French https://www.legifrance.gouv.fr/loda/id/JORFTEXT000037085952) ('the Amendment Law') integrates the GDPR provisions in the existing Act No. 78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties ('the 1978 Act').

The French supervisory body responsible for overseeing and enforcing data protection legislation is the Commission nationale de l'informatique et des libertés (CNIL). It is tasked with monitoring compliance and providing guidance to clarify the 1978 Act. The CNIL often publishes guidelines on its website (https://www.cnil.fr/fr/particulier), mostly in French. Of all the advice provided, the following need to be emphasized as the most relevant guidelines:

- The Six-Step GDPR Compliance Methodology (available in French at *https://www.cnil.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes*);
- Practical factsheets on creating learning databases for artificial intelligence (subject to consultation) (only available in French *https://www.cnil.fr/fr/cloturee-intelligence-artificielle-la-cnil-ouvre-une-consultation-sur-la-constitution-de-bases-de*)
- Recommendations on Data Protection Officers (only available in French at *https://www.cnil.fr/fr/passer-laction/le-deleque-la-protection-des-donnees-dpo*);
- Guidance on ISO 27701 and the Processing of Personal Data or Personally Identifiable Information (only available in French *https://www.cnil.fr/en/iso-27701-international-standard-addressing-personal-data-protection*);
- *Guidelines on Data Protection Impact Assessments ('DPIA') (only available in French https://www.cnil.fr/sites/cnil/files/atoms/files/journal_officiel_de_la_republique_francaise_-_ndeq_326_du_6_novembre_2018.pdf).*

The CNIL has also prepared and made available various tools to assist with and ensure GDPR compliance, such as online forms for personal data breach notifications (only available in French https://notifications.cnil.fr/notifications/index), templates, such as record of processing activities (available https://www.cnil.fr/en/gdpr-toolkit/record-processing-activities), as well as relevant software (e.g. Privacy Impact Assessment Software (available https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment), which contributes to the data protection impact assessments.

Regarding the monitoring of ethical compliance of the research projects and initiatives, in France there are currently 39 Ethics Committees, responsible for assessing the ethical compliance of research initiatives. All the Committees of Protection of Persons (Comités de Protection des Personnes, CPP) in each region have jurisdiction over the whole territory, and simultaneously each committee has a nationwide jurisdiction. As per the Code de la santé publique (Chapter III; Articles L1123-1 to L1123-14), the Ethics Committees have the authority to make decisions about interventional studies, standard of care studies, medicinal and other health goods, and other research topics. In addition to the regional Ethics Committees, there is a National Consultative Ethics Committee (Comité consultatif national d'éthique, CCNE), whose main purpose is not only to identify and address problems that arise from advancements in the field of life sciences, but also to publish public statements and recommendations about these matters. Lastly, the establishment of the National Commission for Research Involving the Human Person (CNRIPH) was mandated by the French legislation on March 5, 2012, and it guarantees the coordination and harmonization of the CPPs' operations, primarily via the formulation of recommendations. (http://www.eurecnet.org/information/france.html).

***Germany***

The GDPR and supplementarily the Federal Data Protection Act of June 30, 2017 (implementing the GDPR) (BDSG, available at https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.pdf), are the governing laws for Germany's data protection system. In Germany, the system of data protection is more complex. More precisely, Germany has a dual-tier structure, with a federal body known as the Federal Commissioner for Data Protection and Freedom of Information (in German: Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit - BfDI) responsible for supervising public bodies and telecommunications. Additionally, there are distinct state agencies that regulate the private sector. The BfDI, serves as Germany's representative in the European Data Protection Board, and it is responsible for handling complaints related to data protection issues amongst various regulatory bodies. The competence for complaints is split among different data protection supervisory authorities in Germany. The relevant competent authorities can be identified according to the list provided under www.bfdi.bund.de/anschriften.

In September 2023, the Federal Ministry of the Interior and Community released a proposed legislation that seeks to modify the BDSG, with a specific emphasis on the work of the German Data Protection Conference (DSK). The DSK, a working group representing the BfDI and several supervisory agencies, has released GDPR guidance notes that provide practical advice on different facets of data protection legislation in Germany (only available in German https://www.bfdi.bund.de/DE/Fachthemen/Gremienarbeit/Datenschutzkonferenz/DSK-tableKurzpapiere.html?nn=253022). These provide helpful practical guidance on several fields, such as:

- Processing activities;
- Sanctions and mandate of supervisory authorities;
- Data transfers to third countries;
- Data Protection Impact Assessments (DPIAs);
- GDPR compliance measures;
- Certification schemes.

Moreover, regarding the ethics compliance mechanisms in Germany, there are 53 research ethics committees, which include entities such as the German Research Foundation (DFG), Federal Ministry of Education and Research (BMBF), and Leopoldina – German National Academy of Sciences. More specifically there are 33 attached to Faculties of Medicine/Universities, 17 attached to Medical Associations ("Ärztekammern") in the States and 3 attached to States governments. These RECs are the only legally competent ethics committees to assess all kind of biomedical research programs. Meanwhile, the Permanent Working Party of Research Ethics Committees in Germany (PWPREC) is the official association of RECs in Germany, representing approximately 85% of all Research Ethics Committees (RECs) in the country.

At a national level, the National Council for Ethics ("Deutscher Ethikrat") http://www.ethikrat.org/ has the authority to deliver non-binding recommendations, whilst the Central Ethics Committee of the German Medical Association offers comments on broader ethical matters and may provide guidance to the Ethics Committees of the Medical Associations at their request. Its advice is also non-binding.

***Greece***

The Hellenic Data Protection Authority (HDPA) is an autonomous administrative public authority in Greece with the mandate to oversee the enforcement of the General Data Protection Regulation (GDPR) and other legislations concerning the safeguarding of persons against the handling of their

personal data. Law 4624/2019 is now in effect as of August 29, 2019. The HDPA, or Hellenic Data Protection Authority, is the official supervisory body in Greece responsible for overseeing the enforcement of data protection legislation inside the country. The primary legal framework comprises the regulations stipulated in the GDPR and the corresponding national legislation. The HDPA adheres to EU guidelines, including those provided by the European Data Protection Board (EDPB). In 2023, the HDPA published several important guidelines concerning the failure to meet the rights of data subjects, the failure to report data breaches, and the violation of HDPA regulations governing the correct installation and operation of CCTV systems. More information can be found here: https://www.dpa.gr/el/enimerwtiko/prakseisArxis

In Greece, ethical monitoring is implemented through a central body- the National Ethics Committee and RECs in all hospitals. More precisely, the REC system in Greece comprises the following committees:

- The National Ethics Committee of the National Organization for Medicines;
- Local RECs at hospitals;
- Local RECs in research centers (e.g., FORTH, BRFAA, and other research institutes);
- Local RECs embedded in HEIs (medical faculties)[3].

The legislative framework for RECs in Greece consists mainly of the following recent Laws in Greece:

1. Law 2071/1992 (NHS): Creation of the National Council for Medical Ethics and Deontology.
2. Data Protection Act 2472/1997
3. Act 2667/1998: National Bioethics Commission
4. The Act 2619/1998: Ratifying the Oviedo Convention
5. Adaptation of Directive 2001/20/EE by Decision DYG3/89292/31.12.2003 publ., EK No 184 Annex
6. Act 3418/2005: Code of Medical Ethics and Deontology

Lastly, while the Law on Research and Technology Act 3653/2008 specifies how research protocols should be evaluated, it does not refer directly to what role Ethics Committees have in this evaluation.[4]

***Hungary***

The primary legislation in Hungary regarding the protection of personal data is Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information, which was modified by Act XXXVIII of 2018. The National Authority for Data Protection and Freedom of Information (NAIH) oversees the implementation of this legislation, which establishes the overall structure for safeguarding data. The NAIH is charged with overseeing and advancing the implementation of two essential rights: the right to personal data protection and the right to freedom of information. Additionally, it promotes the unrestricted flow of personal data throughout the European Union. Prior to the implementation of the GDPR, the NAIH released a guideline that delineates the 12 most crucial obligations for ensuring GDPR compliance. More information can be found https://naih.hu/kiadvanyok-publikaciok).

[3] More information available at http://earthnet.ntua.gr/research-ethicsresearch-integrity-committees-in-greece/?lang=en

[4] http://www.eurecnet.org/information/greece.html

In Hungary, the ethics committees of the Medical Research Council (ETT) are comprised of the following committees: the National Ethics Committee for Clinical Pharmacology (KFEB), the National Ethics Committee for Human Reproduction (HRB), and the National Scientific and Ethical Committee (TUKEB). Additionally, there are 10 Regional Scientific and Ethical Committees (RKEBs) that have the responsibility of evaluating local or regional biomedical research, including research projects, clinical trials, and studies undertaken by graduate and postgraduate students. Lastly, Institutional Research Ethics Committees (IKEBs) are present at all institutions conducting clinical trials. These committees ensure that all conditions for research adhere to Good Clinical Practice (GCP) and other appropriate resources and principles. It should be further mentioned that according to the Health Care Act, all these ethics committees enjoy autonomy and are operating as independent committees.

***Ireland***

In Ireland, the Data Protection Act 2018 implements the GDPR, with the Data Protection Commission (DPC) being the country's national independent authority. The DPC is responsible for ensuring compliance with the GDPR and carries out activities related to other regulatory frameworks, including the ePrivacy Directive and Regulation and the Data Protection Directive in the context of law enforcement. The DPC also engages and is responsible for the settlement of complaints and the implementation of enforcement measures. Moreover, the DPC offers information and guidance for individuals and organizations on several aspects of data protection issues, amongst which are the following: the issuance of guidance on the qualifications required for a Data Protection Officer (DPO) under the GDPR, as well as guidance on DPIAs. The qualifications assistance for a DPO can be found at https://www.dataprotection.ie/en/organisations/know-your-obligations/data-protection-officrs/guidance-appropriate-qualifications, and the DPIA Guide can be accessed at https://www.dataprotection.ie/sites/default/files/uploads/2019-10/Guide%20to%20Data%20Protection%20Impact%20Assessments%20(DPIAs)_Oct19_0.pdf

The National Office for Research Ethics Committees (NRECs) in Ireland is responsible for ethics compliance monitoring in research. Its mission is to safeguard and maintain a robust, safe and transparent research ethics review system that enhances the national research infrastructure and procedures. It should be noted that a crucial component of the NREC system is the need to provide nationally recognized ethics decisions, sometimes referred to as a 'single national ethics opinion'. The NRECs collaborate with local research ethics committees (there are 12 RECs in Ireland), and get assistance from the National Office team to operate within a mixed-model system. Their primary objective is to provide support for research ethics in all areas, and specifically of health research fields in Ireland.

***Italy***

The GDPR has been implemented in Italy by amendments to the Italian Personal Data Protection Code (the Code), as specified in Regulation (EU) 2016/679.

The Italian Data Protection Authority (Garante per la protezione dei dati personali) is the governing body responsible for overseeing and enforcing the GDPR and the Code. It is an independent authority established to safeguard fundamental rights and freedoms related to the processing and collection of personal data, as well as ensuring the preservation of individuals' dignity. One of its main tasks is to handle complaints from individuals about their personal data. It also supervises the implementation of data protection measures by organizations that collect and process data. Additionally, it creates and shares recommendations to help companies comply with laws related to the protection of

personal data. The 'Garante' has issued a comprehensive guidance on the implementation of the GDPR, which can be accessed in Italian at this link:

https://www.garanteprivacy.it/regolamentoue/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali

Additionally, the 'Garante' has published several other helpful guidelines, which are available in Italian at this link: https://www.garanteprivacy.it/normativa-e-provvedimenti/provvedimenti/linee-guida.

Regarding the formation and operation of ethics committees in Italy, Law n.3/2018 enabled a major reform of ethics committees in light of the implementation of Regulation (EU) 536/2014. This law, in particular, establishes 40 territorial ethics committees with Decree 26 January 2023[5]. More specifically, ethics committees are responsible for ensuring the rights, safety, and well-being of those undergoing trials, as well as providing a public assurance of such protection. The Law No. 3/2018 also establishes the National Coordination Centre of Local Ethics Committees for Clinical Trials Concerning Medicinal Products for Human Use and Medical Devices, which coordinates, guides, and monitors the activities of analysing the ethical aspects of clinical trials on medical goods for human use, that are entrusted to territorial ethics committees. (https://www.aifa.gov.it/en/centro-coordinamento-comitati-etici).

Lastly, there is also the Ethics Committee (EC) of the Italian National Institute of Health (ISS), which is a body tasked with guiding and evaluating research and experimentation from an ethical standpoint, in accordance with current legislation, and in the context of monitoring research and clinical trial protocols in accordance with the principles recognized by the main research ethics declarations at the international level, as well as current legislation. (https://www.iss.it/web/iss-en/ethics-committee1)

***Luxembourg***

In Luxembourg, data protection is governed primarily by the GDPR and, in addition, by the Act of August 1, 2018, on the Organization of the National Commission for Data Protection and Implementing the GDPR, which contains very few exceptions to the GDPR. This Act essentially supplements the GDPR and defines the roles and responsibilities of the National Commission for Data Protection (Commission Nationale pour la Protection des Données (CNPD)).

The CNPD is the national supervisory authority under Article 51 of the GDPR, and it is in charge of overseeing and ensuring the GDPR's application in Luxembourg, as well as advising the government and other institutional bodies on legislative matters concerning the protection of data subjects' rights in Luxembourg.

Furthermore, the CNPD has issued a number of guidelines in recent years (guidelines can be found at https://cnpd.public.lu/en.html), and in addition to those guidelines, the CNPD provides more general guidance on its website for both data subjects and professionals.

In addition to the CNPD, a number of other authorities, professional associations, and orders advise their members on GDPR compliance.

[5] Available at: https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2023-02-%2007&atto.codiceRedazionale=23A00852&elenco30giorni=true

Furthermore, in Luxembourg, there is a single national clinical research ethical committee: the Comité National d'Ethique de Recherche (CNER). The ethics committee, meanwhile, is liaising with the CNPD, having a member at its meetings as an observer. This Committee gives a single opinion which is valid for all the sites in the country. Opinions issued by CNER during its meetings are provided to the CNPD and Competent Authority (Pharmacy and Medicines Division of Ministry of Health) that will give authorization when due. Furthermore, the ethics committee also tries to establish links and contacts with different research centres on a voluntary basis.

More details can be found at CNER website at: https://cner.gouvernement.lu/fr.html.

***The Netherlands***

The Netherlands is primarily governed by the GDPR and the Dutch GDPR Implementation Act (the Act) when it comes to the processing of personal data. The Dutch Data Protection Authority (Autoriteit Persoonsgegevens - AP) is the relevant supervisory authority, which is increasingly active in providing guidance and enforcing regulations. The AP frequently cites the guidelines issued by the European Data Protection Board (EDPB) and also publishes its own guidelines, Q&A's, and explanations on various subjects related to the GDPR and the Act.

The website of the AP (https://autoriteitpersoonsgegevens.nl) also offers guidance specifically on the use of artificial intelligence (AI) and algorithms. These guidelines are available only in Dutch at https://autoriteitpersoonsgegevens.nl/themas/algoritmes-ai.

The Netherlands also has a total of 24 MREC's (Medical Research Ethics Committees) that are officially recognized and responsible for evaluating and assessing medical and scientific research inquiries and projects. Most of them are associated with an institution, such as an academic medical centre or a hospital. Any research that falls within the purview of the Medical Research Involving Human Subjects Act must be presented to a recognized MREC for authorization prior to its implementation.

The Central Committee on Research Involving Human Subjects (CCMO), also known as the Centrale Commissie Mensgebonden Onderzoek in Dutch, sometimes functions as the MREC (Medical Research Ethics Committee). The MREC evaluates procedures in compliance with the regulations specified in the Dutch legislation, namely the Medical Research Involving Human Subjects Act (WMO).

The Central Committee (CCMO) is furthermore responsible for accrediting MREC's. If an MREC ceases to meet the requirements, the CCMO has the authority to revoke its certification. For research initiatives in the Netherlands, including multicentre research, just one decision from an approved MREC is necessary. More information about the work and the procedures of the CCMO can be found at this link: https://english.ccmo.nl/mrecs/accredited-mrecs

***Norway***

Norway's privacy framework is governed by the Personal Data Act of June 15, 2018, which integrates and implements the rules of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679). The Act, in conjunction with Regulation 0563/2018 on the Processing of Personal Data, incorporates specific national modifications and supplements to the GDPR. The Norwegian data protection authority, known as 'Datatilsynet' (https://www.datatilsynet.no/en/), is responsible for supervising and enforcing data protection laws in Norway. Datatilsynet maintained its substantial oversight efforts and issued major decisions during 2021 and 2022. The Datatilsynet has released guidance pertaining to the following areas (only available in Norwegian):

- Data protection and digital attacks (available at https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/avvik/digitale-angrep/);
- Data breaches (available at https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/avvik/);
- Legal basis for processing (available at https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/om-behandlingsgrunnlag/);
- Codes of conduct (available at https://www.datatilsynet.no/regelverk-og-verktoy/atferdsnorm/);
- DPIAs (available at https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdering-av-personvernkonsekvenser/);
- AI and Privacy (available at https://www.datatilsynet.no/regelverk-og-verktoy/rapporter-og-utredninger/kunstig-intelligens/).

Additional useful guidelines can be found available here: https://www.datatilsynet.no/en/.

***Poland***

Poland's data protection framework is regulated by the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') and the Act of May 10, 2018, on the Protection of Personal Data. This legislation primarily governs procedural matters, including:

- The requirement for public entities to appoint a data protection officer (DPO);
- The obligation to notify the appointment of a DPO;
- The validation of an organization with the authority to issue certification;
- The organizations with the authority to oversee codes of conduct and certification;
- The endorsement of a set of rules for conduct;

The powers of the Polish Data Protection Authority (Urząd Ochrony Danych Osobowych – UODO, , https://uodo.gov.pl.) are also regulated by the Act of May 10, 2018, on the Protection of Personal Data. The UODO, which stands for the Office for Personal Data Protection, serves as the national supervisory body in Poland. Its main role is to oversee the effective enforcement of the General Data Protection Regulation (GDPR) and other relevant data protection laws in the country. The UODO has issued a number of guidelines, with the most notable ones being:

- Guidelines on implementing a risk-based approach;
- The updated list of data processing activities that require a Data Protection Impact Assessment (available only in Polish at https://archiwum.uodo.gov.pl/pl/424);
- Comprehensive guidance for maintaining records using templates for both the record of processing activities and the record of all categories of processing activities conducted on behalf of a controller, including examples of completed templates;
- Detailed guidelines outlining the responsibilities of controllers in relation to data breaches.

In Poland, the system of ethical compliance comprises several committees that are classified as advisory bodies to the Ministry of Science and Higher Education and national ethics committees. The former include the Panel on Principles of Conducting Scientific Research in Biomedicine, the Panel for Molecular Genetic Research and Biobanking, and the Convent of Disciplinary Officers, among others. In addition, there are national ethical committees, such as Regional Bioethics committees. These committees are located inside regional medical chambers, medical institutions, and medical research and development organizations. These committees have a vital function in evaluating ethics, namely in the domains of biomedicine, molecular genetic research, and animal experimentation.

***Spain***

The GDPR has been enacted through the Organic Law 3/2018 of 5 December, which focuses on safeguarding personal data and ensuring digital rights, known as the LOPDGDD.

The Agencia Española de Protección de Datos (AEPD) is Spain's competent national regulatory body responsible for overseeing data protection. It also serves as the representative for Spain on the EDPB. Regional Data Protection Commissioners are responsible for overseeing the processing of personal data by regional public authorities and other entities that are under the control of regional public authorities.

Nevertheless, the AEPD has absolute autonomy from the Public Administration and is responsible for disseminating information about its operations and safeguarding individuals' right to personal data protection. It has released numerous significant guidelines, including those pertaining to the following issues:

- Risk Management and Impact Assessment in the Processing of Personal Data (*https://www.aepd.es/guides/risk-management-and-impact-assessment-in-processing-personal-data.pdf*)
- Guidelines on the compliance with the duty to inform (available in Spanish https://www.aepd.es/sites/default/files/2019-11/guia-modelo-clausula-informativa.pdf);
- Guidance on the drafting of contracts between controllers and processors (only available in Spanish https://www.aepd.es/sites/default/files/2019-10/guia-directrices-contratos.pdf);
- Guide for the DPO certification scheme (only available in Spanish https://www.aepd.es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/delegado-de-proteccion-de-datos/certificacion) ('the Certification Scheme Guidelines');
- Guidelines on the adaptation and incorporation of processing operations integrating Artificial Intelligence to the GDPR (only available in Spanish https://www.aepd.es/guias/adecuacion-rgpd-ia.pdf);
- Requirements for Audits of Treatments that include IA (only available in Spanish *https://www.aepd.es/guias/requisitos-auditorias-tratamientos-incluyan-ia.pdf*);
- Guidelines on the validation of cryptographic systems in data protection (only available in Spanish https://www.aepd.es/guias/orientaciones-criptografia-aepd-isms-apep.pdf)

There is also an approach to data spaces from a GDPR perspective, which can be found in Spanish at the following link: https://www.aepd.es/guias/aproximacion-espacios-datos-rgpd.pdf.

In addition, the AEPD has released various tools to facilitate compliance with the GDPR. These tools can be accessed at the following link (only available in Spanish): https://www.aepd.es/guias-y-herramientas/herramientas.

In Spain, there are also about 140 Ethics Committees (ECs), mainly focused on biomedical research. They are divided into two kinds of ethics committees, namely the Ethics Committees for Investigation (CEI) (32 committees accredited as CEI) and the Research Ethics Committees with Medicines (CEIm) (over 90 committees accredited as CEIm), which are responsible for overseeing, evaluating, and guaranteeing the performance of the research projects. Both kinds of committees are competent for safeguarding the rights of the research projects and clinical trials' subjects and guaranteeing public assurance by issuing opinions on the relevant documentation of the projects, according to the provisions of Royal Decree 1090/2015.

More information can be found at: http://archive.eurecnet.org/information/spain.html.

***Sweden***

The Swedish Authority for Privacy Protection (Swedish: Integritetsskyddsmyndigheten - IMY), formerly the Swedish Data Protection Authority (Swedish: Datainspektionen), is a Swedish government agency, organized under the Ministry of Justice, which constitutes the competent supervisory authority in Sweden, responsible for issues concerning data protection. IMY's main role is to safeguard the individual's privacy in the current information age by monitoring and inspecting the effective enforcement of the pertaining data protection legislation applicable in Sweden, as well as by issuing guidelines and legal opinions on data protection matters. IMY regularly issues guidelines, mainly through articles on its website, that can be found here: https://www.imy.se/en/.

It also issues legal opinions (only available in Swedish at: https://www.imy.se/om-oss/aktuellt-fran-oss/oversikt-praxisbeslut/rattsliga-stallningstaganden/).

***Switzerland***

In Switzerland, the protection of personal data is established by Article 13 of the Federal Constitution. This article states that "(1) every person has the right to privacy in their private and family life and in their home, and in relation to their mail and telecommunications and (2) every person has the right to be protected against the misuse of their personal data". Another important text is the Federal Act on Data Protection (FADP), in force since 1 July 1993. The corresponding ordinance (DPO) regulates the details. Other laws at a cantonal level contain numerous provisions which further specify the requirements associated to personal data protection. A new version of the FADP has been also defined to better align the Swiss dispositions with those contained in the GDPR. It was approved by the Swiss Federal Parliament on 27 September 2020 and is expected to come into force in 2022. The authority in charge of the application of the personal data protection legislation is the Federal Data Protection and Information Commissioner.' The latter is considered as national contact point for the project, if questions should occur in regard to personal data protection in relation with activities in Switzerland.

The Federal Data Protection and Information Commissioner has made available an information centre with relevant guidance, templates, factsheets, and other useful information in the following site: https://www.edoeb.admin.ch/edoeb/en/home/deredoeb/infothek/infothek-ds.html

# 3 Legal considerations

This section introduces all relevant legal requirements that are of relevance to the SLICES infrastructure, with the aim to ease the implementation of due diligence and compliance activities in the future while addressing evolving legal requirements.

This section presents a high-level overview of the information, while Annex 1 provides a more in-depth analysis of the information provided herein.

## 3.1 Research and innovation

Given its nature as a research infrastructure and its main funding sources, the SLICES-RI is bound to meet public dispositions on FAIR (Findable, Accessible, Interoperable, Reusable) and open data, ensuring the generation of social benefits, and aligning with managerial policies and procedures

associated with publicly funded research and innovation activities, which are detailed in specific guidance and documentation generated by the European Commission. Such requirements are encompassed in various regulations, including the following:

- Digital Europe Programme Regulation (EU) 2021/694
- Horizon Europe Regulation 2021/695

### 3.2 Industrial policy

In regard to Industrial Policy, there are several regulations that are applicable to the SLICES project. These regulations, while sometimes only tangentially relevant to SLICES, have been taken into due consideration in order to ensure the project is in line with the standardized approaches of the industry. The identified regulations and normative documents related to the industry are listed below and further elaborated upon in the mapping that has been conducted for the SLICES legal framework (Annex 1):

- InvestEU Programme Regulation (EU) 2021/523
- Recovery and Resilience Facility Regulation (EU) 2021/241
- Regulation on High Performance Computing Joint Undertaking (EU) 2021/1173
- Connecting Europe Facility Regulation (EU) 2021/1153
- Decision on a path to the digital decade (EU) 2022/2481
- Community legal framework for a European Research Infrastructure Consortium (ERIC) (EC) 723/2009

### 3.3 Data and privacy

As the very nature of SLICES requires the handling of data, as an inextricable element of research activities, respecting privacy and data protection regulations is essential to the success of the project and its proliferation as a key research infrastructure in Europe and beyond. As further elaborated in the Data Management Plan, SLICES is committed to demonstrating due diligence and utmost care when processing and handling any personal data, while adopting an "as open as possible, as closed as necessary" policy. Through this dual approach, SLICES is promoting innovation and open dissemination of knowledge while respecting individuals' privacy.

As such, the following data-related regulations have been particularly considered for the design and implementation of the SLICES legal framework:

- *Open Data Directive (EU) 2019/1024*: promoting the data minimization principle of 'as open as possible and as closed as necessary'
- Regulation (EU) 2016/679 (General Data Protection Regulation - GDPR): the main instrument for personal data protection in the EU
- Directive 2002/58/EC on Privacy and Electronic Communications
- Regulation (EU) 2018/1725 on the free flow of non-personal data
- Regulation (EU) 2022/868 (Data Governance Act - DGA)
- Regulation (EU) 2023/2854 (Data Act)

### 3.4 Intellectual property rights

Given the nature of the SLICES infrastructure, tools, and solutions, intellectual property rights are a key consideration for its legal framework. Intellectual property rights ensure the proper management

and protection of innovative work and solutions. In the context of SLICES, such rights may emerge both during the infrastructure's design and implementation phase, as well as through the use of the SLICES ecosystem. As such, SLICES has considered from the start all relevant dispositions regarding intellectual property so as to balance such rights with Open Science requirements, including the following:

- Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society (InfoSoc Directive);
- Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC,
- Directive 96/9/EC on the legal protection of databases (Database Directive).

### 3.5 Cybersecurity

As already highlighted, SLICES is envisioned to assume a central role in the research community, positioning itself as a leading research infrastructure. Such a role is accompanied by increased obligations to ensure the provision of secured solutions, with a particular focus on cybersecurity. In order to ensure a high level of cybersecurity, SLICES has considered the following legislative and regulatory requirements, exploring potential certification avenues and further liaising with key stakeholders:

- Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)
- Proposal COM/2023/208 for a Regulation amending Regulation (EU) 2019/881 as regards managed security services
- Regulation (EU) 2021/887 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres
- Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

### 3.6 Trust and safety

A crucial requirement for the widespread adoption of the SLICES solutions is fostering trust with end-users and citizens whose lives may be affected by the use of the SLICES infrastructure. With that in mind, SLICES has focused from the start on building robust, safe and trustworthy systems and solutions, including when Artificial Intelligence solutions are involved, adopting existing standards, but also exploring further liaisons with European standardization bodies to propose the adoption of standards identified in the course of its activities. The following legislation, along with the standards described below, have been of increased relevance to that end:

- Regulation (EU) 2012/1025 on European Standardization
- Proposal COM/2021/206 for a Regulation laying down harmonised rules on Artificial Intelligence (AI Act)

### 3.7 Commerce and consumer protection

In alignment with the above need for trustworthy and safe solutions, SLICES has prioritized the protection of its end-users as consumers, albeit not in the traditional sense. By incorporating such consideration in its legal framework, SLICES is in the position to provide services of higher quality and afford a greater extent of protection over its end-users, rendering its value proposition more appealing. In order to achieve those objectives, it has particularly considered the following legislation:

- Regulation (EU) 2018/302 on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market (Geo-Blocking Regulation);
- Directive (EU) 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services (Digital Content Directive).

### 3.8 Relevant standards

To complement and better understand potential ways of operationalization of the ethical and legal requirements, the project carried out an additional mapping (Annex 2) focused on relevant standards. The following is a synthesis of the main elements of relevance:

- ISO/IEC 27001 Information Security Management

Companies of all sizes and in all industries can benefit from the guidance provided by the ISO/IEC 27001 standard for setting up, implementing, maintaining, and continuously enhancing an information security management system (*ISO/IEC 27001*, n.d.). In the context of SLICES, the project focuses heavily on data integrity, confidentiality, and resilience as well as Information and Communications Technology (ICT) and information security management.

- ISO/IEC 20000 Information Technology (IT) Service Management

ISO/IEC 20000 aims to provide an overview of how to apply ISO/IEC 20000-1/higher service management maturity level requirements and how to leverage other standards and frameworks to assist with Service Management Systems' implementation (*ISO/IEC 20000 IT Service Management – A Practical Guide*, 2021). An effective ICT service management system is essential to a dispersed research infrastructure such as SLICES, especially when taking legal frameworks' criteria for end-user/customer satisfaction into account.

- ISO/IEC 2382 Information Technology Vocabulary

This vocabulary standard, which is derived from the multi-part ISO/IEC 2382 standard, is meant to make international information technology communication easier (*ISO/IEC 2382*, n.d.). It is given in a language-specific order. It provides definitions and terminologies for a few key concepts related to this discipline in two languages. The definitions are written with the intention of avoiding any linguistic quirks in order to translate into other languages easier. Harmonization of terminology, definitions, and vocabulary used is paramount for SLICES, in order to duly standardize its operations.

- ISO/IEC 30141 Internet of Things Reference Architecture

Using shared terminology, reusable designs, and industry best practices, this document offers a standardized IoT Reference Architecture (*ISO/IEC 30141*, n.d.). It takes a top-down approach, starting with gathering the most crucial IoT features, abstracting them into a general IoT Conceptual Model, and using that model to create a high-level system-based reference before breaking it down into five distinct architectural views. To facilitate deployment and experimentation, this standard plays a major role whenever integration of IoT-related services or infrastructures is being considered in SLICES.

- ISO/IEC 17788 Cloud Computing Overview

The standard defines keywords and an outline of cloud computing (*ISO/IEC 17788*, n.d.). It serves as the foundational vocabulary for cloud computing standards and is applicable to different organization types. The relevance of said standard is evident considering that SLICES leverages cloud technologies and envisions an automated RI as a Service (RiaaS).

- ISO/IEC 38500 IT Governance

The governing bodies of organizations, including partners, owners, directors, executive managers etc, can utilize ISO/IEC 38500:2015 as a guide when it comes to the appropriate, effective, and efficient use of IT in their businesses (*ISO/IEC 38500*, n.d.). The governance of the organization's present and future use of IT, including management procedures and choices pertaining to that usage, is governed by ISO/IEC 38500:2015. In the context of SLICES, it is the executive director that will be responsible for representing the project and carrying out the supervisory board's decisions, as stated in Article 16 of the SLICES Statutes (*SLICES-PP Statutes*, 2024).

- IEC 62443 Security for Industrial Automation and Control Systems

As a fundamental component of automated cybersecurity, shared responsibility is a foundational idea of the ISA/IEC 62443 standards (*ISA/IEC 62443 Series of Standards - ISA*, n.d.). In order to guarantee the security, dependability, integrity, and safety of control systems, cooperation of stakeholder groups is key. SLICES' community of researchers and use of cutting-edge digital technologies place this standard's cybersecurity requirements into practice.

- IEC 62264 Enterprise-Control System Integration

The standard's objectives are to lower the risk, expense, and error associated with creating system interfaces and to improve the uniformity and consistency of interface language (*IEC 62264-1*, n.d.). SLICES operational safety is guaranteed through the integration by design and by default of cybersecurity and data protection considerations.

- IEC 61508 Functional Safety

IEC 615008 offers functional safety requirements for the lifetime of products and systems that are electrical, electronic, or programmable electronic (E/E/PE) (*IEC 61508 Functional Safety Standard*, n.d.). It focuses on the components of an apparatus or system—such as sensors, actuators, control logic, and microprocessors—that carry out automated safety tasks. It offers a strict quantitative method for lowering risk and is applicable to a wide range of sectors. SLICES is expected to accomplish its objective in over ten research infrastructures. Modern infrastructures are equipped with IoT, cloud, and wireless technologies, all of which were developed with the systems' functional safety in mind.

- ITU-T Y.2060 Overview of the Internet of Things

In addition to outlining the IoT reference model, this standard also defines the concept and extent of the Internet of Things and points out its essential traits and upper-level specifications. Additionally, an educational supplement contains the ecosystem and business concepts. Since the project's progress entails the use of IoT, this standard overview offers essential guidance on how to use IoT.

- ITU-T Y.3001 Future Networks

The design aims and objectives for future networks (FNs) are outlined in ITU-T Y.3001 (*Y.3001 : Future Networks: Objectives and Design Goals*, n.d.).

Four goals—service awareness, data awareness, environmental awareness, and social and economic awareness—have been established to set FNs apart from other networks. Twelve design goals have been identified to achieve these goals: network management, mobility, identification, reliability, and security; virtualization of resources; data access; energy consumption; service universalization;

economic incentives; and service diversity. In order to standardize APIs, SLICES is fully aligned with the objectives and activities related to FNs and is in communication with ITU and IEEE to that end.

- ITU-T X.805 Security Architecture for Systems Providing End-to-End Communications

In order to provide end-to-end network security, this recommendation specifies a network security architecture (*X.805 : Security Architecture for Systems Providing End-to-End Communications*, n.d.). The general security-related architectural components that are required to provide end-to-end security are defined in this recommendation and have been taken into consideration when designing the SLICES infrastructure and related solutions.

- ITU-T Y.3501 Cloud Computing Framework

By outlining the fundamental prerequisites for cloud computing, this recommendation offers a foundation for cloud computing (*Y.3501 : Cloud Computing - Framework and High-Level Requirements*, n.d.), including Infrastructure as a Service (IaaS), Network as a Service (NaaS), and Platform as a Service (PaaS). The standard is of high priority for the SLICES Infrastructure and future actions given the nature of the activities performed and envisioned.

- W3C WebRTC Standard

In order to enable the sending and receiving of media and generic application data to and from another browser or device that is implementing the necessary set of real-time protocols, this document specifies a set of ECMAScript APIs in WebIDL (*WebRTC: Real-Time Communication in Browsers*, n.d.). In order to gain access to local media devices, this specification is being developed in tandem with an API specification and a protocol specification created by the IETF RTCWEB group. Providing a network for researchers to enhance their studies through improved databases, infrastructure, and communication is one of SLICES's objectives, so the ECMAScript is considered when input is exchanged over audio and video channels.

- W3C Web of Things (WoT)

By utilizing and expanding on current, standardized Web technologies, the Web of Things (WoT) aims to prevent the Internet of Things from becoming more fragmented (*Home - Web of Things (WoT)*, n.d.). W3C WoT facilitates seamless integration between various IoT platforms and application domains by offering standardized metadata and other reusable technological building blocks. The standard supports the SLICES ERIC's objectives for a unified research infrastructure that standardizes IoT data.

- W3C RDF Standard

RDF expands the Web's linking structure (*RDF - Semantic Web Standards*, n.d.), rendering it possible to combine, expose, and share structured and semi-structured data across many applications. Due to its role in data interoperability, the standard is a useful tool for academics interacting with data within the SLICES infrastructure.

- W3C OWL Standard

OWL is a language based on computational logic, meaning that computer programs can use the knowledge represented in it to make implicit knowledge explicit or to check for consistency (*OWL - Semantic Web Standards*, n.d.). Ontologies, or Open Knowledge documents, are able to be published on the World Wide Web and can link to or be linked from other OWL ontologies. The data description could benefit from the use of this language. Semantic web language is required for the project development since all training activities will be designed with multilingual assistance and cultural sensitivity in mind to attract participants from a range of backgrounds.

- ETSI EN 303 645 Cyber Security for Consumer Internet of Things

The consumer IoT devices that are connected to network infrastructure (such the Internet or home network) and their interactions with related services are covered by the high-level security and data protection rules outlined in this document (*Cyber Security for Consumer Internet of Things: Baseline Requirements*, 2020). This does not include the related services. The following is not an exhaustive list of examples of consumer IoT devices: smart cameras, TVs, and speakers; wearable health trackers; connected home automation and alarm systems, especially their gateways and hubs; connected appliances, like washing machines and refrigerators; connected smoke detectors, door locks, and window sensors; IoT gateways, base stations, and hubs to which multiple devices connect). Furthermore, security issues unique to limited devices are covered in this document. SLICES will put the required safeguards in place to ensure cybersecurity and data protection. Among these will be data erasure when it's no longer required, anonymization, pseudonymization, and protection by design and default.

- ETSI Network Functions Virtualization (NFV)

The NFV architecture framework, functional components and their interfaces, virtualization requirements, protocols and APIs for these interfaces are all described and specified in the standards (*NFV*, n.d.). The format and organization of deployment templates, as well as the manner in which all artifacts utilized by the NFV management and orchestration framework should be packaged, are specified by an additional set of NFV requirements. Through the broad usage of Network Functions Virtualization (NFV), a repository of ready-to-deploy experiments will be built, allowing users to expand, duplicate, and fork an experiment to fit their needs. The FAIR standards will be followed while disclosing the results.

- CEN/CENELEC EN 50600 Data Centre Facilities and Infrastructure

The standards allow specific data centre essential infrastructures to be categorized as having a certain degree of availability' (*Energy Management and Environmental Viability of Data Centres*, 2021). These designations are used in EN 50600-1 to define an overall "availability" level. Other standards in the series do not designate a "availability" level; instead, they just demand compliance to a set of requirements. Concerns concerning "certification" to these standards and how they stack up against competing third-party methods are frequently raised the management of data centres will take into account the energy efficiency and ecological goals of EU policy. These will be accomplished both internally by the design of the centres and externally by the tests.

- NIST Special Publication 800-53

This publication offers an inventory of security and privacy controls for information systems and organizations to safeguard against a variety of threats and risks, such as hostile attacks, human error, natural disasters, structural failures, foreign intelligence entities, and privacy risks, as well as organizational operations and assets, individuals, other organizations, and the country (Force, 2020). The controls are applied as a part of an organization-wide risk management strategy and are adaptable and adjustable. SLICES has taken all these elements into account in order to ensure a robust system upholding cybersecurity and privacy standards.

- Europrivacy – European Data Protection Seal

The EDPB has officially approved Europrivacy as the first European Data Protection Seal, enabling its use to evaluate and verify compliance with the GDPR and related national data protection laws for all types of data processing (*Europrivacy Certification*, n.d.). Through it, candidates may better understand and manage their risks, show and value their compliance, and improve their reputation

and access to markets. SLICES can benefit from the Europrivacy compliance assessment methodology (www.europrivacy.com).

## 4 Socio-economic considerations

In regard to the effect on the market, SLICES RI is expected to 'continue to support existing jobs and promote new employment opportunities in science, research and development fields as well as supporting exchange of knowledge and expertise on a local level due to financial and technological constraints'(*Socio-Economic Ex Ante Impact Study of the SLICES RI*, n.d.). Thus, through the research infrastructure, new employment opportunities will be created, which will, in turn, benefit the market.

An example of how SLICES-RI will have an effect on the job market is through 'intra-European mobility'. As such, the SLICES infrastructure could attract skilled specialized personnel from third countries assisting the advancement of technological developments and the market as a whole. The latter will, for example, have an impact on competition, which is a major driving force of the market, both within the European Union and internationally. Such a European research infrastructure is 'essential' for European research, as it will allow researchers and academics to conduct experimentation. Thus, European economic stakeholders will gain a competitive advantage early on in the development process, as 'experimentation is key to validate scientific concepts and assess and qualify diverse design assumptions and choices under realistic conditions'.

Another concrete example of how the SLICES infrastructure can affect the market is its predicted impact on smaller-sized businesses and market entry. The infrastructure could promote and facilitate the digital transition and, thus, lower the costs for start-ups and small businesses to enter the market and compete with bigger companies. Hence, those businesses can afford to stay in the market longer and develop their products leading to valuable output (*Socio-Economic Ex Ante Impact Study of the SLICES RI*, n.d.). SLICES Deliverable D3.1 outlines a robust human resources policy. Targeted effects of SLICES include the development of the local economy and innovation environment, as well as economic growth through industry and SMEs support.

In addition, businesses will be further supported and will be able to reduce costs thanks to the tests of cutting-edge technologies. These technologies will be tested and developed in a safe and trustworthy environment thanks to SLICES which will prepare businesses for their usage in the future.

However, SLICES will not only have an impact on competition between countries on a national level, but it can also contribute to the mitigation of social and economic imbalances in the European Union, allowing Member States to have equal access to a larger united European infrastructure and markets for lower costs. This will be the case through the involvement of various stakeholders, such as experts, researchers, public institutions, and industries. Therefore, local economies will thrive through new employment opportunities and shared insights from other countries and companies. Thus, fragmentation will be combatted by the SLICES Infrastructure through the access to the shared research platform, data, and knowledge about technologies that can help advance the economy.

Moreover, SLICES is in line with the European Open Science Cloud and the European Digital Market policy. The creation of a unified research infrastructure system will contribute to the initiatives and the growth of the European market economy through the increase of Gross Domestic Product (GDP) in the ICT domain. This is a response to the competition with US and Chinese major industry players. SLICES will expand its influence on the telecom market as well and with this will boost investments. In turn, the establishment of a single RI will lead to a scalable and adjustable configuration.

Thus, the European member states have the chance to become more competitive in the digital world thanks to the SLICES infrastructure. The SLICES Infrastructure will 'provide wider and faster access to data-based and cloud-based data processing services, which will allow a pan-European business to become more digitalized and standardized (*Socio-Economic Ex Ante Impact Study of the SLICES RI*, n.d.). Therefore, European companies will be better equipped to compete in the international digital market with, for example, American companies. SLICES will provide the opportunity to promote the European software and application industry on international markets. SLICES will help to advance in this sense 'following a European and international technology roadmap'. This roadmap includes 'the Union's Digital Strategy and Horizon Europe Cluster 4, future PPPs, the new 5G flagships, 6G developments and the output of many European projects', but will also allow a 'link to international initiatives such as US NSF PAWR and FABRIC'.

SLICES will also enhance cyber-security and, thus, help industries to be protected and resilient to external threats. This can have a beneficial outcome for the market, as cyber-crime can decrease the efficiency of the digital market. Additionally, the SLICES RI can also help to protect democratic values within the European market by protecting national security, which leads to the preservation of the free-market structure and economic prosperity on a national and European level.

Overall, the SLICES Infrastructure is able to 'supply European industries with all necessary tools to address relevant market needs, regional regulations and global challenges' (*Socio-Economic Ex Ante Impact Study of the SLICES RI*, n.d.). Furthermore, it can contribute to the achievement of the Horizon 2020 objectives by knowledge sharing and exchange of R&D.

### 4.1 Market analysis and business model implications

In order to have a better understanding of the expectations and needs of the industry, the SLICES Consortium conducted a survey under the aegis of the SLICES-PP project.

This survey was based on a 10-question interview (available in Annex 3) which was discussed with respondents preferably in person. Inputs from 20 companies from 10 different countries were received, covering 70% of the countries participating in the consortium (*SLICES-PP Results of the Industry Interview*, n.d.).

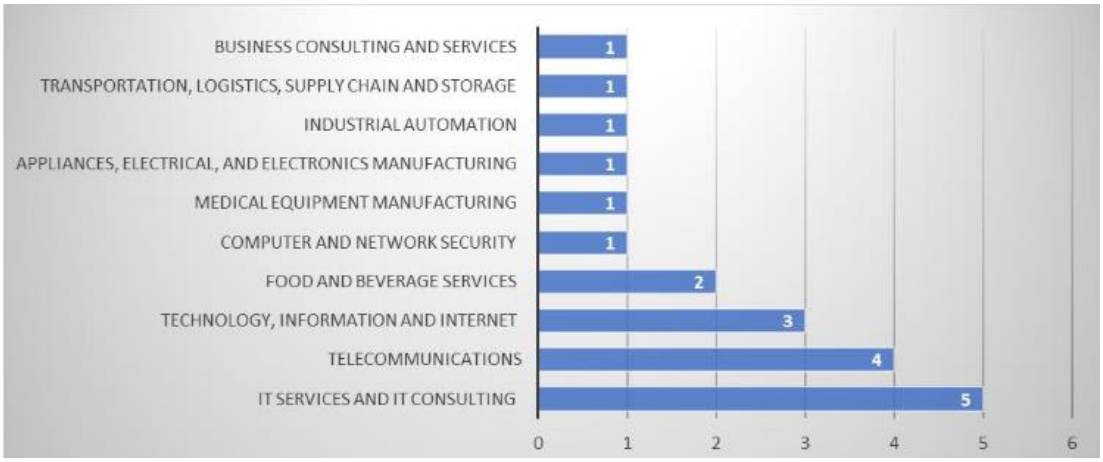



Figure 3. Distribution of Responders Organizations by Industry

For the sake of analysis, we present below some of the relevant outcomes of the survey carried out in SLICES-PP.

Overall, when identifying the exploitable assets, our respondents highlighted that SLICES RI grants them access to knowledge and provides a ground for further research on various domains. Access to experimental data was highly appreciated and the possibility of technological exploration and collaboration and being connected with other groups, laboratories and their facilities were praised. This feedback reinforces our community-building approach around SLICES-RI.

In light of elaborating upon the economic effect that SLICES will have on the industry, the industry interviews that have been conducted are valuable indicators of the economic value that SLICES will bring. Those interviews revealed, for example, that the RI and scientific software tools seem to be the most valuable exploitable assets for industrial SLICES users (*SLICES-PP Results of the Industry Interview*, n.d.). This can be seen at hand of the results of the answers to Question 1, which are shown below.

Q1. Please rate the following Exploitable Assets (EAS) SLICES is providing. 1 meaning least valuable, 5 meaning most valuable for your company.

a. Research Infrastructure
b. Scientific Software Tools
c. Scientific Hardware Tools
d. Experimental Data

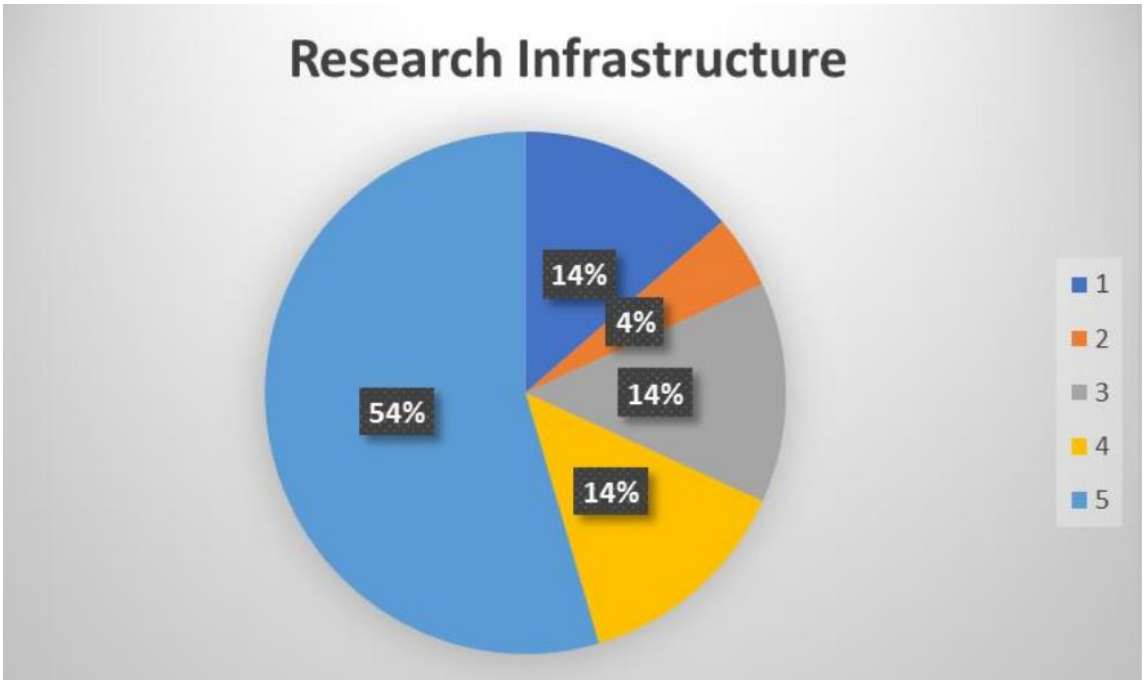



Figure 4. Value of research infrastructure for industrial SLICES users

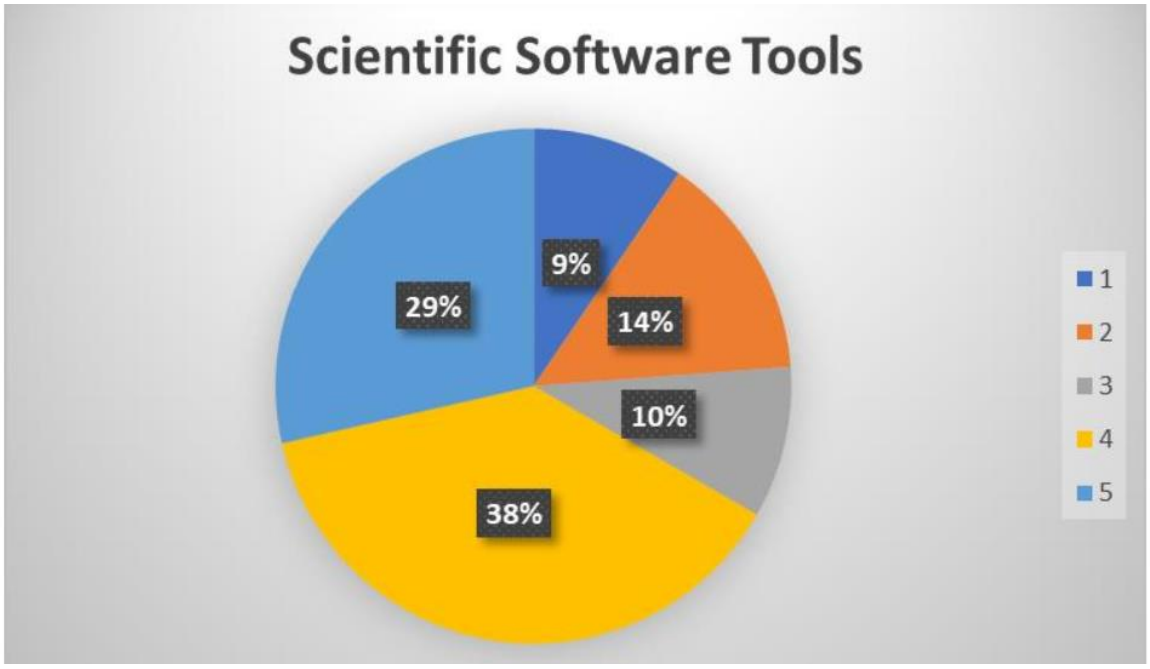



Figure 5. Value of scientific software tools for industrial SLICES users

In general, participants of the industry interviews were asked to identify those exploitable assets that would be most valuable for them as stakeholders in the industry. The list below shows the different exploitable assets that were mentioned in Question 2.

- Simplified access to and use state-of-the-art high-performance research infrastructure and special scientific hardware tools
- Access to open source software components
- Access to knowledge
- Provides a ground for further research on various domain
- Develop new solutions utilizing new network concepts
- Improve products
- Testing to determine the limitations of our products in terms of scalability and performance
- Testing on large scales (efficiently)
- Using of heterogenous infrastructure (e.g. Cloud mixed with cellular/wifi)
- Reproducibility of real-life and/or artificial (but reproduceable) test conditions
- Testing in near real-world conditions, or testing a reduced model and complementing the testing and evaluation with simulation based on the reduced model behaviour
- Testing in a physical test setup to increase product reliability
- Access to specialized hardware, ability to quickly test new ideas.
- Conduct experiments
- Cloud robotics, distributed multi-agent research, training and testing complex digital twins, machine learning, specialized use case synthetic data set generation and training, performance testing of our robots using wireless testbeds
- Running large-scale experiments
- Opportunity to federate the BI-REX local testbed (IoT devices, local edge cloud nodes, private 5G cell, ...) With the SLICES distributed testbed

- Obtain feedback and data about the usage of state-of-the-art software tools for such deployment environments
- Experimental data about energy consumption of the many equipment involved in such geo distributed infrastructures
- Technological exploration and collaboration and being connected with other groups, laboratories and their facilities
- Opportunities of research & development collaborations
- Experiences from different set ups, private network if any, robotics, experimental industry, references for own business, slicing results for new technologies, utilize the network and contacts for own research project, to find competencies to areas where we do not have competences, seminars, presentations, trainings
- Scientific Software Tools: Standardized, scientifically-proven tools, description of experiment workflows including a preferably automated evaluation and preparation of benchmarking results
- Scientific Software Tools: Benchmarks with a solid scientific foundation
- Utilization of end-to-end services, such as localized weather forecasting, yield estimation.
- Development of new innovative products and services.

Additionally, in Question 3 of the industry interviews, participants were asked of any additional exploitable assets, that exceeds the list of categories given to participants. The list below, which is a summary of the answers to this question, illustrates additional valuable benefits that industry partners see in SLICES.

- Security guarantee: a guarantee that nobody else can access the company data that is uploaded into the cloud. This is usually not available when using a research infrastructure. There should be a properly audited solution to guarantee this. Amazon has some solution for this, at least that is more transparent. (Suggested workaround: upload encrypted or standardized data.)
- Additional computational resources for data analytics
- Manufacturing data, quality assurance, image processing, fault detecting
- Simulations, though most tools are not mature yet to make use of the cloud/be used in a cloud environment
- Global logistics models
- Sharing of experience, best practice is also a good method to benefit in organizing new experiments.
- Cloud: virtual wall
- Wireless Wi-Fi & 5G
- Real world operational warehouse infrastructure.
- Having blueprints or best practice descriptions that can accelerate the practical deployment of real testbeds
- Experience sharing, discussion forums with practical elements about software versions, installation issues that were not expected, …
- Standardisation, Recommendations ITU/ETSI ...no only research results but turning them to clear concrete standards and product requirements
- Education assets. Development of own personnel
- We are interested in novel, state-of-the-art techniques and procedures in information technology. As a company, we can directly profit from training activities teaching these

techniques and procedures. However, we can also benefit from hiring people that were academically educated on state-of-the-art IT procedures and tools.

- SLICES-RI could be used as a teaching facility for the next generation of IT experts. Such a testbed can provide server-grade hardware for academic research and education offering state-of-the-art systems. Nowadays, students are mostly trained on virtual machines with limited resources. If teaching is based on real hardware that is closer to the systems used in a real data center students can acquire competencies that cannot be easily achieved using the virtualized environments. Two important competences for us are the ability to estimate system performance, i.e., how much bandwidth can be handled by a server. Another important aspect is the ability to estimate the scalability of applications, i.e., what is the bottleneck of a specific application.
- Collaboration with partners across Europe and beyond, exchange of ideas, participation in joint research and innovation proposals.
- Improving relationship and networking between industry and academia research groups.
- Specific synergies with research partners.

There are several further insights that can be gained from the industry interviews, giving a better insight into the business model that SLICES is pursuing. As such, for example, the answers to whether stakeholders would be willing to pay for the SLICES RI (answer to Question 4 of the industry interviews) were overwhelmingly positive with 75% answering 'yes or possibly' (*SLICES-PP Results of the Industry Interview*, n.d.). Additionally, the answer to Question 7 was positive as well, namely 'the majority of the industrial SLICES users find the current application and project evaluation process and schedule feasible and acceptable. There were some interesting ideas and advice, which could be worth considering'. A last mentionable point, which gives an insight into the business model of SLICES, would be the answers of the industry partners to Q10. As such, the majority of the partners would be interested in participating in face-to-face training, workshops, or online training either in real-time or on-demand in the future.

### 4.2 Connections with social elements (Green Deal, energy efficiency, climate neutrality, technological sovereignty, security, and inclusion) and link with EC agenda

In regard to the social aspects and benefits that SLICES will bring to the table for consumers and citizens in general, there are several aspects to be highlighted. The SLICES project intends to address a large and diverse community of users in regard to geographical location, background, and industrial involvement. As such, SLICES will bring about a large societal impact.

Firstly, as SLICES RI is creating an interconnected net of European research data, including scientific and experimental resources, the European industry and the various stakeholders will be better equipped to conform to the needs of customers and European citizens. Hence, SLICES RI will provide the opportunity to better address social challenges throughout Europe as a united front. An example of this is the twin transition to a sustainable and digital economy.

SLICES is also focused on education and training, therefore, improving the lives of citizens by enhancing their employability and knowledge. The project will 'provide an innovation lifelong educational opportunity for students, researchers and engineers, who will have access to remote experimental on equipment, which is often not available locally'. Thus, through education, SLICES will bring equality regarding learning materials and other such issues related to education. This may help to improve the overall life quality of affected citizens while directly addressing the digital divide.

Lastly, the technological advantages, which will 'allow to develop new frontier technologies in a better, faster and cheaper way than ever before' are having a direct effect on citizens as the costs of these services go down as well as entry barriers to the market are lowered. These advantages stimulate collaboration and openness about innovation, thus, leading to the lowering of costs for companies in the market. This effect is likely to be passed on to the consumers, who then directly benefit from lower costs through innovation. Furthermore, by integrating SLICES RI, 'the European companies will have better chances to improve their presence and competitiveness in biotechnology, software and hardware, where R&D is a leading factor'. This incentivizes new companies to join the market and contribute to these innovations, as well as engaging young researchers and PhD students that will benefit from education and training.

***Green Deal***

The European Green Deal is one of the responses of the European Commission to combat climate change and environmental degradation (*The European Green Deal – European Commission*, 2021). The European Green Deal presents a set of policies whose aim is to ensure that net emissions of greenhouses are cut down to 55% by 2030 and completely phased out by 2050. In addition, it is a green transition that will foster modern economic development as well as technological advancement, change and growth (*European Green Deal*, n.d.). For this reason, the Green Deal covers policies in several sectors such as transport, energy efficiency, climate, industry, sustainable finance and agriculture. Each initiative of the package plays a different role in achieving the desired goals. For example, the Fit for 55 translates the initiative to reduce greenhouse emissions until 2030 by 55% into a legal obligation for the European Members (*Fit for 55 – The EU's Plan for a Green Transition*, n.d.).

Besides making it legally mandatory, the European Green Deal initiatives follow established values. These are cost-efficiency, socially fair transition, climate resilience, nature-based solutions, civil protection, preserving biodiversity, affordability, sustainability, and strengthening industry competitiveness (*European Green Deal*, n.d.). In order to do so, the European Commission has proposed a shift to a circular economy, which secures sustainable products, consumer empowerment, and waste reduction. Moreover, a circular economy means that European Union institutions, industry players and scientific researchers act together to achieve the desired goals. Studies show that the collaboration between the public and the private sector can contribute to the sustainability and decarbonization of 20% of CO2 emissions (Malmodin & Bergmark, 2015).

The aims of the European Green Deal are closely related to the purpose of SLICES-SC, SLICES-PP and SLICES-RI. The realization of these projects is in line with the Green Deal objectives as they promote digitalization, technological advancement and change, which will contribute to public-private collaboration (UDGA, 2024). In continuation, the SLICES projects will connect research infrastructures, such as the IoT Lab in Geneva, Switzerland, which follow the strategy of the International Declaration on IoT for Sustainable Development and the 17 Sustainable Development Goals adopted by the United Nations (UDGA, 2024). 8 of the SDGs have a focus on nano- and digital technologies, and share the values of the European Green Deal, including: Good Health and well-being; Quality Education; Affordable and Clean Energy; Industry, Innovation and Infrastructure; Sustainable Cities and Communities; Responsible Consumption and Production; Climate Action; Partnership for the Goals (UDGA, 2024).

Thus, by promoting the creation of a shared European Research Infrastructure, participating facilities and institutions will be able to increase their complementarity capabilities and harmonize to contribute to the Green Deal objectives. Additionally, through the exploitation of SLICES research

facilities, the projects will be able to share knowledge and resources across various domains to create sustainable solutions and generate economic growth, technological development, efficient use of energy, agriculture and industry innovations.

***Energy Efficiency***

Energy efficiency has been declared as one of the goals in the European Green Deal and in the 17 Sustainable Development Goals adopted by the United Nations. In terms of the Green Deal, energy efficiency is observed in the transition to energy-efficient housing, reducing energy poverty, building clean energy infrastructures with the help of EU energy corridors, using renewable- and climate-neutral sources, and integrating energy systems. The transition to energy efficiency in these fields will lead to economic growth and technological development and contribute to standardization. The creation of energy sectors will also improve the fight against heat loss and harmonize greener electricity among end-use sectors, such as transportation, industry, and homes. Moreover, the European Commission introduced in 2009 a Renewable Energy Directive that should increase the usage of energy from renewable sources to 45% (*Renewable Energy Directive*, n.d.). The seventh goal of the United Nations' SDGs has a similar standard as the European Green Deal. It aims to secure energy that is sustainable, accessible to everyone, modern, and reliable (*THE 17 GOALS | Sustainable Development*, n.d.).

By providing solutions in line with the European Green Deal and energy consumption, SLICES aspires to become a leading solution for AI in Digital Sciences with its functioning regulated according to the ESFRI White Paper. SLICES-SC will achieve the objective of energy efficiency through the connection of research partners who operate closely with sustainable energy. For example, UTH contributes to the SDGs by implementing a NITOS infrastructure and using it for experimentation. The NITOS infrastructure reduces energy consumption through energy harvesting and conducts experiments that make use of clean energy. Inria, the French National Institute for Research in Digital Science and Technology, commits to the SDG objectives by researching new energy sources and energy consumption of data centers. IMT in France runs a testbed on the influence of energy on Dis, effective management of power and thermal energy and inclusion of energy from renewable sources. Their research aims to generate solutions for sustainable cities and increase energy from renewable sources. SLICES-SC also provides a data center where researchers can carry out experiments and monitor and optimize their consumption.

The SLICES-RI has the potential to further enhance its energy efficiency through internal energy audits to measure progress and advise on energy-saving practices, encompassing architectural design and interoperability solutions. By bringing together institutes and researchers and providing an environment to implement energy-efficient practices, SLICES-SC contributes to the European Green Deal and to the SDGs on energy efficiency. SLICES-SC allows for joint research activities and green research infrastructures where specific actions will be undertaken by WP3: Landscape Analysis for Sustainability and Impact Reduction (surveying, assessing and managing RI efficiency); Architecture and Requirements Specification for Sustainable RI (conducting studies and evaluating energy efficiency); Technology enablers for energy-efficient, reproducible Open Science (creation of a machine-learning based model to lower energy consumption).

***Climate neutrality***

The European Commission strives to become the first climate-neutral continent through a set of policies. For this purpose, the EC has undertaken several initiatives, including the EU Green Deal, the

Green Digital Charter (*Green Digital Charter - GuiDanCe*, 2017) and the FIRE EU Initiative (*FIRE+ (Future Internet Research & Experimentation) | Programme | H2020*, n.d.). The EU Green Deal provides a main initiative for reaching climate neutrality, which will be achieved through various means: enforcing legal obligations, creating a shift in food systems for more sustainable models (Farm to Fork Strategy), promoting growth, change and innovation in the European industry for a green digital transformation, circular systems of production and consumption, low-carbon economy, and modernization of the energy sector (*European Green Deal*, n.d.). More specific actions of the EC for the achievement of climate neutrality include investment in environmentally friendly technologies, investment in research and development, and international cooperation to improve standards around the world (*5 Facts about the EU's Goal of Climate Neutrality*, n.d.).

SLICES will promote climate neutrality in different ways. First, the implementation of SLICES-RI will support standardization among research infrastructures in Europe, a necessary step towards a greater shared impact on continental goals for climate neutrality. The above-mentioned objectives will be better implemented through the creation of a shared European Research Infrastructure to contribute to carbon-neutral smart city solutions and low-investment cost innovations. Second, SLICES-SC presents a solution to sustainable usage of resources with less carbon emissions as a result of the increase in digital and telecommunications technologies. SLICES-SC is also in line with many of the European Green Deal objectives, as it connects a community of researchers with industry stakeholders to enable communication, exchange of information, and boost innovation. Better innovation helps pave the path for energy-efficient technologies with reduced carbon emissions to realize climate neutrality goals.

***Technological sovereignty***

Technological sovereignty within the borders of Europe is understood as the prevention of circumstances where Europe is dependent on a limited number of third-world country suppliers of technologies (Statement to Accompany the Launch of the Full EIC, 2021). At the same time, technological sovereignty means that innovators and researchers are stimulated to scale up on global markets and attract more investors from stable countries or use the technology we have in Europe. To do so, the EIC combines national and EU policies from different fields on competition, defence, and industry. Moreover, the EIC actively supports start-ups and projects that have the potential to become leading technologies in the relevant fields.

SLICES-SC contributes to the goal of technological sovereignty through the development and deployment of EU-driven technological infrastructure solutions for research, which it further supports by means of its education and training activities. This aim is the fourth target of the 17 Sustainable Development Goals adopted by the United Nations. Accordingly, members of the UN have set out the goal to provide quality education and continuous learning opportunities for everyone. The SLICES infrastructure will allow for better communication between research facilities and for a long-term strategy for training services. With this, SLICES-SC also contributes to the achievement of the SDGs.

Moreover, SLICES will stimulate knowledge transfer between academic communities, which will lead to the development of EU-sovereign ICT solutions. This will be done in two stages. First, SLICES-SC facilitates the exchange of materials in core technologies, such as cloud-native networking and high-performance computing. SLICES training courses are developed where university researchers, students, and EU ICT industry representatives are educated further. The second stage of the initiative focuses on providing study materials to train users of the RI, which will help coordination between researchers and industry partners to conduct experiments. Furthermore, SLICES is in line with the EIC

pilot Advisory Board on technological sovereignty. It performs the objectives set out in the Digital Single Market for the creation of a European Open Science Cloud (*European Open Science Cloud (EOSC) - European Commission*, 2023). SLICES-SC will connect several European entities, which participate in the project for an EOSC so that data, democracy, and integrity are well-protected. These include the International Data Space Association (IDSA) or the GAIA-X European cloud, which compete with Chinese cloud leaders. Technological and data sovereignty are also closely related to ensuring a better security of the data.

***Security***

Technological advancement can be achieved when the researchers can operate in safe conditions where they can experiment and work on disruptive Dis. In order to verify scientific theories, researchers must conduct experiments on the reliability of the foundation and technology behind distributed systems and the Future Internet. This stage of development is the best time for European stakeholders to gain a competitive advantage. Thus, the success, effectiveness, and safety of these technologies have to be proven. SLICES-SC protects the work of researchers by undertaking an all-encompassing approach that combines computing, storage, IoT resources, and networking. This way partners in the project have all of the necessary conditions to conduct their research in a secure and trustable environment. SLICES-RI will bolster these actions by introducing collaborative know-how on the topic from the various infrastructure providers which will feed into the project's results. In particular, SLICES-SC will make use of platforms such as GENI, Fed4FIRE, Fabric, CloudLab, and PlanetLab which are known to be innovative technologies with strong security developments.

Moreover, SLICES-SC does not provide security only within the RIs but also externally through the network of partners. It is important to note that the stakeholders in the SLICES project are initiatives that support research in not only big data but also security. Such are, for example, the International Data Space Association (IDSA) and GAIA-X European cloud which work on the technological sovereignty of European data by further developments. With such a network and by completing its objective to be inclusive and sustainable, SLICES-RI and SLICES-SC infrastructure works on cyber-security tools that are vital for economic growth and the protection of the society within European borders. Not only that, but the benefit of the network of RIs, which SLICES-SC builds, is seen also in the enhancement of testbeds variety to continue research in future projects .

Another domain where SLICES-RI will ensure security is in the collection, processing, and retention of data (UCLAN, 2023). All data will be gathered with the intention of managing the project and only for what is needed in compliance with legal requirements. Furthermore, SLICES-RI will ensure that the data from the experiments, open calls, and the SLICES-SC Web portal is protected according to the relevant policies set out in the Data Management Plan.

***Inclusion***

SLICES contributes to the inclusion of various stakeholders through its wide reach of connectivity. Inclusive growth has been identified in the Europe 2020 strategy as one of the three main priorities to foster social and territorial cohesion. The other two, which SLICES-SC also follows, are smart growth and sustainable growth, connected to technological sovereignty. The project supports the development of the European economy by establishing a research community, consisting of various stakeholders, all of which support innovation to the benefit of the consumer. Moreover, the research community advances digital infrastructures and future technologies. This is in line with the objectives of the European Research Area (ERA) whose aim is to endorse scientific research, innovation and unity

among the relevant stakeholders. In addition, SLICES-SC promotes sustainable growth as it promotes the UN SDGs and the European Green Deal.

To support inclusive growth, SLICES provides valuable access to cutting-edge research infrastructures, a diverse pool of experts, and collaboration opportunities with the purpose of actively supporting researchers and fostering collaboration on a continental scale. SLICES aspires to empower researchers to navigate the complexities of contemporary research effectively.

Furthermore, SLICES-SC is inclusive not only of the researchers and industry players who are responsible for the sustainable and innovative progress in Europe, but also of the users. The governance structure of the initiative adheres to the practices of different research initiatives, such as the ESFRI Ris and its specifications that are made specific to the prerequisites of SLICES. The governance structure is founded on the principles of governance and distributed RI. With a robust Users Committee, SLICES aspires to be user-centric and this way inclusive of an important additional group of stakeholders. The structure of the governance facilitates any action that could further the Sustainable Development Goals (SDG) of the United Nations. The SDGs are furthered both externally, through the experiments that the RI's users conduct, and internally through the creation of the RI.

***Links with EC agenda***

The EC agenda is made according to the goal of transitioning into a sustainable and digital economy. Moreover, the Commission's Research Area Policy Agenda (ERA Policy Agenda) specifies further the goals for 2022-2024 (European Commission. Directorate General for Research and Innovation., 2022). Accordingly, the Union should deepen a truly functioning internal market for knowledge, face the challenges by the twin green and digital transition, and involve society more in the actions, facilitate access to research and innovation, and develop further existing reforms and investments (European Commission. Directorate General for Research and Innovation., 2022). In addition, European statistics show that the ICT sector brought about 6% of the gross value added in 2021 (*ICT Sector: Value Added Stood at 5.5% in 2021 - Eurostat*, n.d.). A fully operational Digital single market can enhance competition, and innovation and boost economic growth as it can add up to €415 billion annually.

The network of RIs that SLICES builds will be able to participate and contribute to this market growth. The creation of a single RI will allow for economically efficient infrastructure. Over time, such infrastructure will become less and less costly while also lowering the overall public spending in this domain. Additionally, SLICES will lower the barriers to entry into the research and experimentation fields for SMEs or other organizations. This in turn will influence positively training and education. Researchers from various fields will be able to exchange experiences in smart cities, eHealth, IoT, smart grid, and many other domains. As it can be seen from previous social impacts, SLICES is also in line with the Commission's Research Area Policy Agenda, as it builds on innovation, increases users' participation in governance, and facilitates the education and training of researchers and students as part of the process to ensure technological sovereignty. Not only that, but all of its actions are in accordance with the European Green Deal and the 17 Sustainable Development Goals adopted by the United Nations for a green and innovative transition.

## 5 Compliance approach and guidance for future developments

The following sections seek to provide general information on the path taken so far by the project to meet the requirements and elements identified across this document, while identifying administrative compliance and due diligence actions of relevance to the SLICES ERIC in the future.

### 5.1 Compliance approach

The SLICES-RI interim governance process has led to the definition of an initial memorandum of understanding which enshrines baseline terms and conditions of relevance to governance activities within the project, including considerations to the effective management, monitoring and compliance of processed data with legal and ethical principles. This approach is further restated in the draft policies that have been prepared thus far for the implementation of the upcoming ERIC, which address the following topics:

- *Access policy (for users):* which requires service requirements, including vis-à-vis monitoring, alignment with standards, open-source software, and transparency requirements with regards to platform requirements and associated measures;
- *Data policies:* which seeks to establish a Data Governance Committee including multiple stakeholder representatives, and addressing ownership, stewardship, accountability, analytics and decision-making while addressing compliance with data collection, processing, planning, quality control, training and education;
- *Decommissioning policies:* detailing coherent decommissioning processes for the infrastructure and headquarters;
- *Dissemination policies:* addressing the need to bolster adoption and awareness of the SLICES-RI and encouraging open science actions, particularly in line with relevant dissemination channels;
- *Employment policies:* Recognizing equal opportunity employment within the SLICES ERIC, as well as non-discriminatory and standardized HR processes;
- *Ethical policies:* Mapping SLICES-RI activities with the principles of integrity, transparency, respect for persons, justice, non-maleficence, and lawfulness while detailing internal ethics committees and alignment with relevant authorities;
- *Policies to address intellectual property rights:* which details the obligation to implement an IPR policy directed to the identification, allocation, protection, management and maintenance of such rights, as well as with technology transfer activities;
- *Personal data protection policies:* they introduce the compliance elements associated with the GDPR requirements (legal basis, issues surrounding special categories of data, data subject rights, responsibilities of Slices when serving as a data controller, joint controller and data processor, security of processing, data breach management, DPIAs, DPO and international transfers of personal data);
- *Procurement policies:* following relevant EU legislation for procurement and public tenders, it follows the principles of transparency, proportionality, mutual recognition, equal treatment, competition and non-discrimination;
- *Scientific evaluation policies:* which establishes the need to define scientific evaluation policies, including regular participation of the International Scientific Advisory Board and details its contents

Together with other relevant documents, these policies seek to establish a comprehensive background to manage compliance with regulatory and ethical requirements in the scope of the ERIC's activities.

In the context of SLICES-SC, compliance elements are also detailed in the Data Management Plan and reproducibility report (D3.2), which provides further clarity on these activities and seeks to further clarify and organize the ethics and data protection-related actions for the SLICES ERIC. In this sense, it proposes the establishment of an independent, Data Protection Office which provides a central hub

for Data Protection-related concerns for data subjects, and which organizes joint compliance activities across SLICES partners. For SLICES-SC, the Data Manager (DM) of the project has also assumed the role of Data Protection Officer (DPO) at the level of the consortium. This role includes ensuring the 'proper and efficient quality management, collection and documentation of the data generated in the framework of SLICES-RI at large, with a special focus on SLICES-SC project' and oversight of the 'conformance of the collected data with the national and international laws, checking that the consortium does not infringe any regulation, and does not disclose sensitive information, including personal data, before publishing.

Additionally, SLICES-SC has sought to ensure a high level of ethical compliance is taken into account. The ethical challenges that come with, for example, developing and providing the large-scale open testbed in the context of SLICES-RI, are recognized and precautions taken by its various stakeholders across its associated projects. Dedicated efforts have been dedicated to ethical challenges, including external viewpoints through interactions with regulators and easing the operationalization of the legal and ethical requirements into data and trust governance models that are tailored to the project. Furthermore, efforts have been introduced to integrate the various expert elements from the SLICES consortium (such as dedicated ethics, cybersecurity or legal departments), into the discussions surrounding compliance, and to integrate whenever viable, the support of external security advisors[6], which is a relevant action for the SLICES RI in the future.

To further support long-term compliance, the following section will introduce relevant actions to be considered by SLICES-RI partners.

### 5.2 Guidance for future developments

In its upcoming phases, the SLICES-RI platform will be required to comply with a series of due diligence and administrative activities stemming from the regulatory and ethical requirements identified in previous sections of this document (and associated with the mapping found in Annex 1 of this deliverable), which include the following:

- Research and Innovation:
  - Data infrastructure development and management in compliance with security and data protection requirements
  - Responsible administration of research data, including consideration of long-term storage of data
  - Integrate transparency, explainability and trustworthiness considerations for any AI solution developed or implemented
  - Monitor implementation and reporting of project-related outputs in alignment with program evaluation guidelines
- Data and Privacy:
  - Handle requests for document and information reuse in a timely manner and in alignment with relevant models, templates and defined processes, including

[6] On this topic, see (SLICES-PP D10.1. EOI – Requirement No. 1, n.d.), which notes that the advisor is 'in charge of monitoring all aspects related to intrusion prevention, event correlation, data flows and use, intellectual property protection' and the position monitors issues connected to the sovereignty of member states and is in charge of assessing the risk of any vigilance leaks connected to SLICES-RI and SLICES-PP.

expediting data identification/exploration and recovery, alignment with relevant principles
    - Grant access to research data at a low (or free of) charge basis when complying with regulatory-based requests, in a non-discriminatory manner
    - Protect personal data processed by design and by default, including:
    - Maintaining records of data processing activities
    - Perform Data Protection Impact Assessments regularly (and prior to new high-risk data processing activities), considering data subject perspectives
    - Define and maintain a network of Data Protection Officers through the SLICES Data Protection Office (see SLICES Data Management Plan).
    - Establish liaisons with relevant data protection authorities at a regional, national and European level, and ensure research infrastructure providers are following their guidance
    - Document compliance at all levels, establishing procedures to ease cross-information of compliance activities and aligning criteria and mitigation measures with relevant tools and solutions (such as the European Data Protection Seal criteria).
    - Establish contractual frameworks to ease data management, data governance and secure international data transfers. Consider relevant certification mechanisms as a means to demonstrate compliance.
- Cybersecurity:
    - Recognize its leading role in regard to research infrastructures and, as such provide an exemplary approach to cybersecurity by:
    - Adhering to and incorporating security-by-design methodologies in regard to data policies
    - Liaising with ENISA in order to support the achievement of a common high-level approach toward cybersecurity across Europe
    - Liaising with the European Cybersecurity Competence Centre in order to engage in international cooperation and influential discussion about the design approach towards cybersecurity policy on a European level.
    - Recognizing its position under ‘other critical sectors’ within the NIS 2 Directive and, thus, approaching the topic of cybersecurity with the utmost care and responsibility.
- Trust and Safety:
    - Engage in standardization activities in order to foster innovation, which will ultimately enhance the trust of end-users and provide a safe platform for research, development and organization.
    - Prioritize, throughout standardization activities, the enhancement of safety for the end-user, sustainability, competitiveness and interoperability.
    - Liaise with relevant European standardization bodies in order to contribute to a strong European network of research and innovation.
    - Comply with and remain aware of regulations that regulate new emerging concepts, such as the AI Act, in order to prioritize the trust and safety of the end-user’s data at any point within the project.
- Intellectual Property:
    - Balance Intellectual Property Rights with the need for Open Science, so as to not limit the publication of the SLICES-SC software unless necessary.
    - Assess whether a stricter approach to Intellectual Property Rights is desirable in certain cases, especially when it could negatively affect the competitiveness of small start-ups and other consortium members.
- Ethics

- Establish liaisons with entities in charge of oversight of ethical compliance at EU or national level, integrating ethics assessment methodologies in the processes, mechanisms and/or policies established by the RI to assign resources and/or enable experiment setup.
- Perform ethical impact assessments to evaluate and mitigate negative affectations generated by SLICES experiments and associated activities, considering in particular the following common principles:
- Governance and oversight:
    - Transparency and openness
    - Trust and governance
    - Research integrity
- Fairness and equity:
    - Fair access and equal participation
    - Justice and fairness
    - Equitable distribution of benefits
- Social responsibility and ethical conduct
    - Social responsibility and gender balance
    - Beneficence and non-maleficence
    - Responsible citizen science
- Responsible innovation and technology
    - Responsible use of technology
    - Responsible innovation
- Sustainability and deviation minimization
    - Sustainability
    - Deviation minimization

# 6 Conclusions

Across its activities, SLICES-SC has sought to advance Europe's digital research infrastructure by fostering a strong community of researchers and developing links with industrial stakeholders, which enables impact generation across multiple socio-economic areas. This being said, the project recognizes that its commitment to advance the state of the art and enable accessible, inclusive and trustworthy research capabilities, can only be achieved with close alignment on ethical and legal compliance between the various stakeholders involved in the development of the SLICES-RI.

This deliverable has supported this alignment by presenting an extensive overview of the relevant dispositions and current actions presented by the project to ensure compliance. It considers country-specific ethical and legal requirements, and emerging administrative requirements, to map the way forward and raise awareness of all stakeholders of the core elements to be considered when developing a successful European Research Infrastructure Consortium.

By minding the proposed activities and aligning stakeholder's perspectives with core ethical principles, the SLICES project can significantly lower the barriers to broader adoption of its solution by key industry and academic players, thus enhancing the impact of the project and fostering collaboration, innovation and technological advancements in line with European goals, practices, and perspectives.

## 7 References


- 5 facts about the EU's goal of climate neutrality. (n.d.). Retrieved 25 April 2024, from https://www.consilium.europa.eu/en/5-facts-eu-climate-neutrality/
- Cyber Security for Consumer Internet of Things: Baseline Requirements. (2020). ETSI.
- Energy Management and Environmental Viability of Data Centres. (2021). The CEN/CENELEC/ETSI Coordination Group on Green Data Centres (CEN/CLC/ETSI CG-GDC)
- EU AI Act: First regulation on artificial intelligence. (2023, June 8). Topics | European Parliament. https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence
- European Commission. Directorate General for Research and Innovation. (2022). European Research Area policy agenda: Overview of actions for the period 2022-2024. Publications Office. https://data.europa.eu/doi/10.2777/52110
- European Green Deal. (n.d.). Retrieved 25 April 2024, from https://www.consilium.europa.eu/en/policies/green-deal/
- European Open Science Cloud (EOSC)—European Commission. (2023, February 10). https://research-and-innovation.ec.europa.eu/strategy/strategy-2020-2024/our-digital-future/open-science/european-open-science-cloud-eosc_en
- European Research Infrastructure Consortium (ERIC). (2023, December 22). https://research-and-innovation.ec.europa.eu/strategy/strategy-2020-2024/our-digital-future/european-research-infrastructures/eric_en
- Europrivacy Certification. (n.d.). Europrivacy Certification. Retrieved 28 June 2024, from https://www.europrivacy.org/en/frontpage
- FIRE+ (Future Internet Research & Experimentation) | Programme | H2020. (n.d.). CORDIS | European Commission. Retrieved 25 April 2024, from https://cordis.europa.eu/programme/id/H2020_ICT-11-2014
- Force, J. T. (2020). Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication (SP) 800-53 Rev. 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5
- Green Digital Charter—GuiDanCe. (2017, January 16). ICTFOOTPRINT.Eu. https://ictfootprint.eu/en/green-digital-charter-guidance
- Home—Web of Things (WoT). (n.d.). Retrieved 28 June 2024, from https://www.w3.org/WoT/
- ICT sector: Value added stood at 5.5% in 2021—Eurostat. (n.d.). Retrieved 26 April 2024, from https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20240423-3
- IEC 61508 Functional Safety Standard. (n.d.). TÜV SÜD. Retrieved 28 June 2024, from https://www.tuvsud.com/en-us/services/functional-safety/iec-61508
- IEC 62264-1:2013. (n.d.). ISO. Retrieved 28 June 2024, from https://www.iso.org/standard/57308.html
- ISA/IEC 62443 Series of Standards—ISA. (n.d.). Isa.Org. Retrieved 28 June 2024, from https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards
- ISO/IEC 2382:2015. (n.d.). ISO. Retrieved 28 June 2024, from https://www.iso.org/standard/63598.html
- ISO/IEC 17788:2014. (n.d.). ISO. Retrieved 28 June 2024, from https://www.iso.org/standard/60544.html
- ISO/IEC 20000 IT service management – A practical guide. (2021, July 6). ISO. https://www.iso.org/publication/PUB100441.html

- ISO/IEC 27001:2022. (n.d.). ISO. Retrieved 28 June 2024, from https://www.iso.org/standard/27001
- ISO/IEC 30141:2018. (n.d.). ISO. Retrieved 28 June 2024, from https://www.iso.org/standard/65695.html
- ISO/IEC 38500:2015. (n.d.). ISO. Retrieved 28 June 2024, from https://www.iso.org/standard/62816.html
- MI. (2023). SLICES Business Plan.
- MI. (2024). SLICES-RI Socio-Economic Ex-Ante Impact Study.
- NFV. (n.d.). ETSI. Retrieved 28 June 2024, from https://www.etsi.org/committee/1427-nfv
- OWL - Semantic Web Standards. (n.d.). Retrieved 28 June 2024, from https://www.w3.org/OWL/
- Radley-Gardner, O., Beale, H., & Zimmermann, R. (Eds.). (2016). Digital Europe Programme Regulation (EU) 2021/694 (2nd ed.). Hart Publishing Ltd. https://doi.org/10.5040/9781782258674
- RDF - Semantic Web Standards. (n.d.). Retrieved 28 June 2024, from https://www.w3.org/RDF/
- Renewable Energy Directive. (n.d.). Retrieved 25 April 2024, from https://energy.ec.europa.eu/topics/renewable-energy/renewable-energy-directive-targets-and-rules/renewable-energy-directive_en
- SLICES-DS D3.4. Final governance structure approved by the partners. (n.d.). Retrieved 6 June 2024
- SLICES-DS_D3.6 Data Protection Policies. (n.d.). Retrieved 7 June 2024, from https://www.slices-ds.eu/wp-content/uploads/2022/12/SLICES-DS_D3.6_approval_disclaimer.pdf
- SLICES-PP D1.1. MoU: SLICES-RI Interim Governance.
- SLICES-PP D7.1. Data Management Plan.
- SLICES-PP D10.1. EOI – Requirement No. 1.
- SLICES-PP Results of the Industry Interview.
- SLICES-RI Interim Supervisory Board (ISB)—Terms of Reference (ToR).
- SLICES-SC D3.1 SLICES-SC Data Management Plan.
- Socio-Economic ex ante Impact Study of the SLICES RI.
- Statement to accompany the launch of the full EIC. (2021). European Innovation Council pilot Advisory Board. https://eic.ec.europa.eu/system/files/2021-03/EIC%20Advisory%20Board%20statement%20at%20launch%20of%20EIC_1.pdf
- THE 17 GOALS | Sustainable Development. (n.d.). Retrieved 25 April 2024, from https://sdgs.un.org/goals
- UCLAN. (2023). SLICES PP D7.1 Data Management Plan.
- WebRTC: Real-Time Communication in Browsers. (n.d.). Retrieved 28 June 2024, from https://www.w3.org/TR/webrtc/
- X.805: Security architecture for systems providing end-to-end communications. (n.d.). Retrieved 28 June 2024, from https://www.itu.int/rec/T-REC-X.805/en
- Y.2060: Overview of the Internet of things. (n.d.). Retrieved 28 June 2024, from https://www.itu.int/rec/T-REC-Y.2060-201206-I
- Y.3001 : Future networks: Objectives and design goals. (n.d.). Retrieved 28 June 2024, from https://www.itu.int/rec/T-REC-Y.3001/en
- Y.3501 : Cloud computing—Framework and high-level requirements. (n.d.). Retrieved 28 June 2024, from https://www.itu.int/rec/T-REC-Y.3501

## Annex 1: Legal framework mapping to SLICES

| Area | Legislation | Key objective(s) | Relevant Provision | Explanation | Relation with SLICES / Relevant SLICES actions. |
|---|---|---|---|---|---|
| Research and Innovation | Digital Europe Programme Regulation (EU) 2021/694 | Fostering of digital transformation of the European economy between 2021-2027 through Union contributions; six specific key objectives<br>- O1: High-Performance computing: create an exascale data center and supercomputing infrastructure accessible to the public and research<br>- O2: Artificial Intelligence (AI): facilitate AI solutions, make them accessible and compliant with data privacy and security<br>- O3: Cybersecurity and trust: procure cybersecurity equipment and deploy security quality measures across the Union | Art. 4, Art. 5, Art, 6, | While not directly connected to SLICES-RI, this regulation enshrines relevant requirements when it comes to cybersecurity, skill generation and public infrastructure. | SLICES aims to build a network that will connect researchers across Europe both in the private and in the public sphere. Their collaborations will lead to better access to results and experiments. As a result, researchers will develop cutting-edge technologies and data will be made available in the entire Union. files, etc. In this context, eventual connection with infrastructures funded under this regulation is of high relevance. |

| | | | | | |
|---|---|---|---|---|---|
| | | - O4: Advanced digital skills: support training and education of digital skills among professionals and students<br>- O5: Deployment and Best Use of Digital capacity and Interoperability: support technological development in the public sectors through the other goals; support industry<br>- O6: Semiconductors: develop semiconductor industry | | | |
| | Horizon Europe Regulation 2021/695 | Facilitate technological and scientific foundations by influencing the Union investment in research and innovation (R&I while maintaining compliance with Union objectives; Four specific objectives.<br>- O1: facilitate scientific knowledge<br>- O2: foster research and innovation while addressing Union | Art. 14 | In accordance with the "FAIR principles," which stand for "findability, accessibility, interoperability, and reusability," responsible administration of research data must be guaranteed. The long-term storage of data will also receive attention. | The SLICES Data Management Plan facilitates the efficient and effective governance of data and makes it available for future investigation, experimentation, and development by other researchers. |

| | | | | | |
|---|---|---|---|---|---|
| | | policies for sustainability, etc.<br>- O3: contribute to technological advancement and innovative solutions<br>- O4: increase Member State's participation and cooperation in R&I | | | |
| Industrial Policy | Recovery and Resilience Facility Regulation (EU) 2021/241 | Bettering crisis responsiveness and growth potential, creating cohesion among MS, supporting Union goals for sustainability and climate targets, upholding social rights, increase renewable energy and security so it fosters an autonomic economy. | Annex VI | Research, development, and innovation are integrated within the scope of the RRF; national recovery and resilience plans should detail measures for public investment in research and innovation and green and digital transitions; and to determine how these responds to economic and social challenges. | While only tangentially relevant to SLICES, the RRF regulation provides baseline references between investment in research infrastructure and its environmental objectives. |
| | InvestEU Programme Regulation (EU) 2021/523 | Investing in policy objectives of the Union to support their development for actions that contribute to: competitiveness, growth the economy, sustainability, innovation, research, education, and crisis responsiveness; 4 specific objectives: | Annex II | The financing and investment operations may include strategic investment to support final recipients whose activities are of strategic importance to the Union, in particular in view of the green and digital transitions, of enhanced resilience and of strengthening strategic value chains. They may include important projects of common European interest. The financing and investment operations may fall under one or more of the following areas: | This regulation showcases the value potential and high-level interest in research infrastructures for the Union. It furthermore presents potentially viable funding avenues for the consortium in line with the project's expected outcomes. |

| | | | | | |
|---|---|---|---|---|---|
| | | - O1: investing in sustainable infrastructure<br>- O2: investing in innovation and standardization<br>- O3: Supporting SMEs and increasing competitiveness<br>- O4: Supporting social investment | | (…) (5) research, development and innovation, in particular through: (a) research and innovation projects that contribute to the objectives of Horizon Europe, including research infrastructure and support to academia | |
| | Connecting Europe Facility Regulation, (EU) 2021/1153 | Developing and standardizing trans-European networks in energy, transport, and digital sectors while contributing to European objectives for sustainability, competitiveness and economic growth; five specific objectives<br>- O1: Contributing to projects for developing transport infrastructures<br>- O2: adopting parts of TEN-T for dual use of transport<br>- O3: Contributing to the development of energy market | Art. 8(2); Art. 8(4)I | Projects in digital connection infrastructure must meet certain objectives and utilize the most suitable and advanced technology. This involves optimizing data flow capacity, ensuring secure transmission, enhancing network resilience, addressing cybersecurity concerns, and achieving cost-effectiveness. Projects that utilize state-of-the-art technology for effective digital platforms are given top priority. These projects also take into account factors such as interoperability, cybersecurity, data protection, and reusability. This strategy guarantees that projects not only fulfil urgent connection requirements but also conform to wider strategic goals and technology norms. | SLICES seeks to enhance European research efforts by creating state-of-the-art technologies that provide cost savings for private market participants. An essential component for promoting innovation in ICT, which is critical for achieving the European economy's sustainability and digital economy objectives, is the establishment of a shared research infrastructure. SLICES will also improve education, training, and the development of skills. The objective of this organization is to offer top-notch services, state-of-the-art technology, and access to a digital research infrastructure for both university and industry. SLICES prioritizes interoperability, dependability, data security, and cybersecurity to enhance the European Research Infrastructure |

| | | | | | |
|---|---|---|---|---|---|
| | | - O4: facilitating cross-border cooperation in energy sector<br>- O5: Facilitating secure and high-capacity networks | | | Area and address user-specific requirements while overcoming existing restrictions. |
| | Regulation on High Performance Computing Joint Undertaking (EU) 2021/1173 | Widening the scope of the regulation to allow for technological developments in AI and supercomputing. Allowing for and ensuring better access to the use of AI in supercomputing for machine-learning and developing the European economy and competitiveness. | Art. 3 | Details the goal of the Joint Undertaking in the development of a demand-oriented user-driven supercomputing, quantum computing, service and data infrastructure which will be federated with EU data spaces and other relevant services | Tangentially relevant, this regulation specifies the potential for interaction between SLICES and the Joint Undertaking envisioned in the Regulation. |
| | Decision on a path to the digital decade (EU) 2022/2481 | Facilitating a digital environment with technologies that support European objectives on sustainability, economy, competitiveness, fundamental rights, inclusivity, openness, equality through continuous education and training. Increasing accessibility to online public services. Making sure that digital infrastructures also comply with the goals above. | Art. 3; Art.4; Art. 11 | Art. 3 establishes the general objectives of the policy programme, which include: “ensuring the Union’s digital sovereignty in an open manner, in particular by secure and accessible digital and data infrastructures capable of efficiently storing, transmitting and processing vast volumes of data that enable other technological developments, supporting the competitiveness and sustainability of the Union’s industry and economy, in particular of SMEs, and the resilience of the Union’s value chains, as well as fostering the | The goal of SLICES-SC is to create and coordinate cooperative training programs for its user community that will support SLICES sustainability and implementation even after the project is finished. Moreover, SLICES supports the goals for a climate-neutral economy, the European Green Deal and a sustainable economy internally through the functioning of the infrastructures, as well as externally through the objectives of the experiments themselves. SLICES is subject to several legislations and initiatives: 17 Sustainable |

| | | | | | |
|---|---|---|---|---|---|
| | | Facilitating communication between public and private, increasing crisis-responsiveness and resilience. | | start-up ecosystem and the smooth functioning of the European digital innovation hubs;" and requires "developing a comprehensive and sustainable ecosystem of interoperable digital infrastructures"<br><br>Art. 4 sets targets for these infrastructures.<br><br>Art. 11 recognizes that: Multi-country projects may be implemented by recourse to any of the following mechanisms: (b) European Research Infrastructure Consortia | Development Goals adopted by the United Nations, the Green Digital Charter, the FIRE EU Initiative, etc. |
| | Community legal framework for a European Research Infrastructure Consortium (ERIC) (EC) 723/2009 | Laying down the requirements and procedures for and the effects of setting-up a European Research Infrastructure Consortium | All | | The core goal of the SLICES-SC project is to support the establishment of the ERIC. |
| | | | Art. 4 | Research infrastructures should meet the requirements for: necessity, added value to ERA, effective access, fostering knowledge and mobility of research, standardizing and disseminating outcomes across Europe | SLICES seeks the establishment of a research infrastructure to enable safer and more accessible experimentation. This in return increases research productivity and innovation which contributed to the development of the European Economy as SLICES will also directly contribute to the ICT value in the EU market. Lastly, SLICES will easy the communication and mobility of researchers and as partners are from different parts, the outcomes of the infrastructure will be disseminated across Europe. |

| | | | | | |
|---|---|---|---|---|---|
| | | | Art. 7 | An ERIC obtains legal personality and status of an international organisations from the day it is established and has the rights of a legal person. | SLICES's establishment date as an ERIC is predicted for 2025 (*SLICES-SC Statutes*, 2024). Moreover, pursuant to Article 2 of the Statutes SLICES will have a statutory seat in France. |
| | | | Art. 10 | ERIC's statues should include at least the article's criteria such as name, seat, activities, duration, list of members, liability regime, basic principles, rights and obligations, working languages, references to statutes. | The statutes describe all of the requirements in the article (*SLICES-SC Statutes*, 2024). |
| | | | Art. 15 | ERIC is primary governance is by Community guidelines and laws supported by national legislation if the matter is not specified by Community law. | SLICES is compliant with the regulatory frameworks listed in this document and table. |
| | | | Art. 17 | ERICs have to create annual activity reports on operations, financial and scientific aspects. The ERIC must inform the Commission if there are any threats and after investigations the ERIC decision can be repealed. | Article 26 of the SLICES statutes stipulates that SLICES will provide an annual report at the end of the Financial Year and will inform the Commission of threats to the ERIC (*SLICES-SC Statutes*, 2024). |
| Data and Privacy | Open Data Directive (PSI), (EU) 2019/1024 | Providing consistent level of protection for data through public security, data protection, making public documents available to the public in safe conditions. Facilitating information | Article 10 | Research data should be made available according to the FAIR principles and the principle of 'as open as possible, as closed as necessary' in relation to intellectual property rights, personal data protection and confidentiality, | SLICES will publish the produced datasets under strict conditions. The information made available via the open data server will be disseminated in accordance with the FAIR principles and connected to the EU's goal for EOSC-II. Moreover, some of the |

| | | | | | |
|---|---|---|---|---|---|
| | | products and services availability across the Union which are based on public documents and free circulation of cross-border information between citizens and industry. | | security and legitimate commercial interests; Research data can be reused if it has already been made public | primary results will be made available to the public in journals and presented in international conferences. Through specific SLICES-SC capabilities, data gathered from the experiments and provided through the portal will be semantically annotated and made available to the public. Along with producing and disseminating FAIR data, SLICES-SC will also link to other significant data repositories such as IEEE Dataport and CRAWDAD (*SLICES-SC Proposal*, 2020). |
| | General Data Protection Regulation (GDPR) (EU) 2016/679 | Protecting natural person's data and fundamental rights, especially to data protection. Setting up rules for free movement of data | Art. 5 | Processing of personal data must be in conformity with the principles listed in Art. 5 GDPR (lawfulness, fairness, transparency, purpose limitation, data quality, data minimization, accuracy, confidentiality, storage limitation, integrity and accountability). | SLICES as an ERIC, must conform to the principles encompassed in Art. 5 GDPR in order to process personal data lawfully. |
| | | | Art. 6(1)(a), 7, 8 | Consent of the data subject can serve as a lawfulness of processing justification. Consent must be documented and there are special requirements for obtaining the consent of minors. | SLICES testbeds provide the necessary information of consent prior to the testbeds' utilization, information shall be provided in a clear and transparent manner, data subjects must be given the choice to clearly consent to the collection and processing of their data by clear affirmative action, the data subject must be given the choice to clearly consent. |

| | | | | | |
|---|---|---|---|---|---|
| | | | Art. 9 | The processing of special categories of data is prohibited, unless an exception is present. Those include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. | Participants are immediately informed about the precise categories of sensitive data and whether they will be processed. Thus, the data subject can make an informed decision in regard to the processing of their sensitive information; A tick box option of the relevant categories of data that are intended to be used can be a viable option to ensure experimenters' full comprehension of data protection requirements and the classification of their experiment within the data protection framework. |
| | | | Arts 12-22 | Under Chapter 3 of the GDPR, data subjects have several rights to ensure that they are treated fairly in regard to the processing activities. Data subjects can exercise these rights at any point in time. | Included in the information that participants and experimenters receive upfront are their obligations and rights regarding data subjects' personal information. |
| | | | Art 25 | The controller must have appropriate technical and organizational measures in place, in order to ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed. | SLICES has adopted a privacy-by-design and by-default approach and, thus, considered data protection and privacy from the very beginning of the project. The SLICES privacy policy is considered for all SLICES steps and throughout its lifecycle to ensure compliance with personal data protection requirements. |



| | | | | | |
|---|---|---|---|---|---|
| | | | Arts 44, 45, 46 | There are specific rules for the transfer of data to third countries. As such, the transfer either needs sufficient appropriate safeguards in the receiving country or an adequate decision by the Commission. | The SLICES Data Policy has already highlighted the SLICES commitment to ensure that any data transfers performed within the SLICES project will be performed in accordance with the standards set out by the GDPR, as well as further EU legislation on the protection of data. |
| | | | Art 32 | Security Requirements: Appropriate access controls must be instated and regularly updated in order to comply with the security of processing. | The SLICES Data Protection Policy has already clarified that access shall be protected by an authentication of user procedure that shall require a username and password, as well as an additional authorization step, while other parties shall be able to view a limited amount of information on the experimenter (e.g. the username). |
| | | | | Awareness and Training: In order to ensure the security of processing, personnel and any person handling the personal data must be trained and aware of certain risks and threats. | The respective Organizations are responsible for training their staff adequately, while staff training activities should effectively communicate SLICES' ethical principles and legal policies. Staff shall be trained on updated legislation and general security routine training. |
| | | | | Audit and Accountability: Since the principle of accountability puts the responsibility on the data controller, the controller shall implement | The testbed's activity will be audited in order to identify potential vulnerabilities, risks and threats |

| | | | | | |
|---|---|---|---|---|---|
| | | | | appropriate technical measures to ensure a level of security appropriate to the risk, this may include regular audits. | |
| | | | | Security Assessment and Authorization: Included in the security of processing is the regular assessment of security measures and authorization methods | 'In order to achieve long-term compliance, it is vital that data protection policies, established procedures and mechanisms, as well as the technical and organizational measures are duly monitored. The project's DPO, in tandem with the DPO network shall be responsible to monitor operations and ensure compliance prerequisites are constantly met.' (*SLICES-DS_D3.6 Data Protection Policies*, n.d.) |
| | | | | Configuration Management: Configuration management is an intrinsic part of the security of processing. | 'Mechanisms should be put in place in case of disturbances provoked by the software or/and the hardware deployed in the SLICES Research Infrastructure. So, the redundancy of the material, applications and networks should be effective and efficient.' (*SLICES-DS_D3.6 Data Protection Policies*, n.d.) |
| | | | | Identification and Authentication: There must be identification and authentication policies in place. | Access is protected through authentication procedures for authorized people only. |
| | | | | Information and document management: There must be | The DPO should record the documentation and information |

| | | | | | |
|---|---|---|---|---|---|
| | | | | effective policies in regard to information documentation in place. | provided by the experimenters for authentication purposes and personal data usage. |
| | | | | Incident Response: There must be effective incident response policies in place. | There are protocols regarding security incidents and breach management, backups and contingency plans should be standardized properly in case of incidents of different natures. |
| | | | | Information system development and maintenance: There must be a maintenance policy in place for the information system, including policies on interoperability and integration. | There are engineers in charge of maintaining the SLICES RI. |
| | | | | Risk management and assessment: There must be a risk assessment strategy and policy in place to best address threats and attacks. | 'Risk of varying likelihood and severity for the rights and freedoms of natural persons posed by the processing: when performing the risk analysis for compliance with Article 25, the risks to the rights of data subjects should be identified. Also, the likelihood and severity of the risks should be determined in order to implement measures to effectively mitigate the identified risks.' |
| | | | | Information system and communication protection/ information integrity/ services acquisition: The organization must have a policy in regard to system and communication protection, | 'SLICES should maintain the data only if the datasets are authentic, reliable and accurate'. (*SLICES-DS_D3.6 Data Protection Policies*, n.d.) |

| | | | | | |
|---|---|---|---|---|---|
| | | | | information integrity and services acquisition | |
| | ePrivacy Directive | Harmonising the rules on fundamental rights and freedoms, especially the right to privacy, to ensure safe personal data processing in the electronic communications sector. | Recital 24, Recital 25, Art. 5 (3) Art. 6, Art. 8, | Devices such as cookies can be used only for legitimate purposes and the user should be made aware of the information about them in a clear and precise manner. Communication electronic networks can only serve as a storage of and access to information when the users are informed about the purposes of processing. Traffic data processing should be limited to certain people who were given the authority to access it but it should be anonymized or erased once it is no longer needed except if it is for billing or interconnection payments. Called users must have the option to block presentations from calling service providers on a per-call basis. Service providers should be informed about this possibility. This applies also to third countries. | Cookies and installation of similar solutions are only allowed with clear information and consent (except for necessary cookies for providing service requested by users from SLICES).<br><br>While SLICES will not fall under the definition of a public communications network, any user-related (or otherwise obtained) traffic and location data should be carefully managed, particularly if the implementation of the SLICES solutions requires the installation of information/software in the user/experimenter's hardware. |
| | Regulation on the free flow of non-personal data (EU) 2018/1725 | Ensuring the free flow of data other than personal data within the Union. Facilitating data economy. | Art. 2, Art. 4, Art. 6 | The regulation applies to the processing of electronic data other than personal data which is given as a service to users within the Union. Self-regulatory codes of conduct should be facilitated and created by all relevant stakeholders based on | If non-personal data is processed, it will be processed lawfully. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | interoperability and transparency and following certain standards. | |
| | Data Governance Act (DGA Regulation) (EU) 2022/868 | Establishing the rules on re-use of certain categories of data by public bodies and creating a supervisory network and notification to provide services on data intermediation. Providing support to exercise rights over these categories of data. Facilitating sufficiently big data pools and enabling machine-learning and data analytics, data altruism. | Recital 25, Art. 6(4) | "scientific research purposes should be understood to include any type of research-related purpose regardless of organizational or financial structure of the research institution in question, with the exception of research that is being conducted by an undertaking with the aim of developing, enhancing standardizing products or services."<br><br>"Where public sector bodies charge fees, they shall take measures to provide incentives for the re-use of the categories of data referred to in Article 3(1) for non-commercial purposes, such as scientific research purposes, and by SMEs and start-ups in accordance with State aid rules. In that regard, public sector bodies may also make the data available at a discounted fee or free of charge, in particular to SMEs and start-ups, civil society and educational establishments." | Discounted fees (or no fees) for certain categories of data for scientific research use should be obtainable from public sector bodies in the context of SLICES-related or enabled research activities |
| | European Data Act (Regulation) (EU) 2023/2854 | Creating equitable access to and use of data in order to support the development of a true internal market for data, as well as making sure | Art. 5, Art. 6, Art. 11, Art. 13. Art. 23, Art. 28, | Data holders with the exception of gatekeepers can share user data with third parties under conditions while keeping trade secrets. Third parties can process the data only for the | The produced data during the project will not be shared with third parties. Thus, although the Data Act will not be directly applicable, the data will be |

| | | | | | |
|---|---|---|---|---|---|
| | | that value from data is distributed fairly across participants in the data economy. | Art. 30, Art.32(1) Art. 33, Art. 35, Art. 41 | determined purposes and erase it when no longer needed. Data holders should undertake the relevant security measures to protect the data according to the laws. Contractual terms that are imposed by one party and are unfair (deviating from good practices) are not legally binding. Consumers should be able to effectively switch to another provider following technical requirements under the Regulation. Data providers have the obligation to make jurisdiction and general description transparent on their websites. Transfer of data internationally to third countries is prohibited if it does not comply with Union laws. Interoperability of data and data sharing should be facilitated. Open interoperability standards should advance technology. Non-binding contractual clauses on computing contracts should be adopted by 2025. | protected under the GDPR and other sources. |
| Intellectual property rights | Database Directive, (EC) 1996/9 | Ensuring that databases are adequately and consistently protected in order to safeguard the compensation of the database creator. | Article 6 | Scientific research is an exception to restricted ads and does not require authorization as long as the source is provided and the non-commercial goal being pursued is sufficiently justified | The Consortium is dedicated to exploitation and understands how crucial it is to the project's success for the licensing schemas to be consistent with the exploitation model (*SLICES-SC Proposal*, 2020). As a result, SLICES-SC will make every effort to publish software as open source, with the exception of a few unique |
| | | | Article 9 | Scientific research is an exception to the sui generis right as long as the | |

| | | | | | |
|---|---|---|---|---|---|
| | | | | source is provided and the non-commercial goal being pursued is sufficiently justified | circumstances where stricter IPR regulations are necessary to enhance the competitiveness of start-ups and SMEs that are consortium members. |
| Cybersecurity | Regulation for a Cybersecurity Act, (EU) 2019/881, 2023/0108(COD) | Raising end users' knowledge of the services and devices securely and encouraging security through privacy and security-by-design at the federal level, strengthening cybersecurity across Europe | Recital 4 | The growth of the cybersecurity sector in the Union, particularly for SMEs and start-ups, is facilitated by ENISA. In order to strengthen supply chains within the Union and lessen reliance on cybersecurity goods and services from outside the Union, ENISA should work to establish deeper partnerships with academic institutions and research organisations. | Liaison with ENISA should be set up by SLICES to increase cooperation and contribute to the reduction of dependence on services from outside the Union and to reinforce supply chains inside the Union. |
| | Regulation to establish a European Cybersecurity Competence Centre (EU) 2021/887 | Bolstering the security of information networks and systems, such as the internet and other vital infrastructures for societal operation. boosting the competitiveness of the Union's cybersecurity industry, maintaining and expanding the Union's technological and industrial capabilities for cybersecurity research | Art. 4(2)(a); Art. 4(3)(a); Art. 5(h); Art. 7, Art. 8 | The Competence Centre has the improvement of cybersecurity and knowledge as an objective through the creation of recommendations and innovation for research. While attempting to prevent the fragmentation and duplication of efforts and replicating good cybersecurity practices, the goal is to facilitate the use of results from research and innovation projects. National coordination centres also have various tasks such as assistance, promoting participation, acting as points of contact, etc. The cybersecurity competence community (multiple stakeholders) | Liaison with the European Cybersecurity Competence Centre Community should be established by SLICES. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | has the task of aiding the centres and the network. | |
| | NIS 2 Directive (EU) 2022/2555 | Enhancing the internal ' market's performance by achieving a common level of cybersecurity. Member States can create separate national cybersecurity objectives under certain conditions. | Art. 2, Art. 7(f) (g), Art. 29, Annex 2 | 6. Member States shall ensure that any natural person responsible for or acting as a legal representative of an essential entity on the basis of the power to represent it, the authority to take decisions on its behalf or the authority to exercise control of it has the power to ensure its compliance with this Directive. Member States shall ensure that it is possible to hold such natural persons liable for breach of their duties to ensure compliance with this Directive. | SLICES does not fall under the essential category, however it does fall under the "other critical sectors" category. As such, SLICES belongs to one of the sectors that are a key enabler to 'successfully embrace the digital transformation and to fully grasp the economic, social and sustainable benefits of digitalization' (preamble 3). |
| Trust and Safety | European Standardization Regulation (EU) 2012/1025 | Establishing European standards and deliverables for standardization for goods and services, including ICT technical specifications, financing European standardization and involving different stakeholders | Art. 5(2), Art. 9 | The participation of relevant stakeholders such as universities and research centres should encourage organisations to facilitate innovation, in particular if the entities are involved in funded research projects. Research facilities of the Commission will contribute to scientific standardization of organization-based safety, security, sustainability, and competitiveness. | SLICES should establish liaisons with European standardization bodies. |
| | AI Act (Regulation), 2021/0106(COD) | Lays down harmonized rules on the use of some AI systems, their deployment on the market, and putting | Preamble 25, Article 2(6), Article 2(8) | The Regulation does not impede research and development activities and promotes innovation and scientific independence. AI models and systems created and | SLICES aims to connect researchers across Europe to increase innovation, boost development and new technologies, and better the European economy. The project does so through |

| | | | | | |
|---|---|---|---|---|---|
| | | into service. It does so to encourage:<br>- the internal market's development, application, and adoption of AI<br>- upholding the highest standards of protection for public interests, including health and safety, the preservation of fundamental rights, such as democracy, the rule of law, and environmental protection, as recognized and safeguarded by Union law<br>- advocating for a European human-centric approach to AI and leading the world in the creation of safe, reliable, and moral AI | | implemented expressly for the aim of furthering scientific research and development are not included in its purview. Furthermore, it guarantees that it won't interfere with scientific research and development efforts related to AI models or systems before they are released or put into use. The rules of this Regulation do not apply to research, testing, or development activities related to product-oriented AI systems or models before those systems or models are put into operation or made available for purchase. | the creation of an ERIC. Moreover, the usage of AI is supposed to generate automatic experiment code generation (*SLICES-SC Proposal*, 2020). Thus, SLICES does not directly fall under the regulation. However, to ensure safety, cybersecurity, transparency and data protection, SLICES will comply with the provisions of the Act. |
| | | | Preamble 69 | The protection of personal data and the right to privacy must be ensured for the duration of an AI system's lifecycle. While processing personal data, the principles of data minimization and data protection by design and by default apply. Measures to guarantee adherence are anonymization and encryption, the use of technology that enables the application of algorithms to the data and facilitates AI system training without data transmission between parties or copies of the raw or structured data itself. | SLICES will follow the requirements set by the Act as well as the GDPR and other legislations in order to secure the safe processing of data. The data used for data input will be anonymized and erased when no longer necessary. |

| | | | | | |
|---|---|---|---|---|---|
| | | | Preamble 75, Article 15(4) | Technical and organisational measures should be taken to ensure the robustness of high-risk AI systems, for example by designing and developing appropriate technical solutions to prevent or minimize harmful or otherwise undesirable behaviour. Those technical solutions may include for instance mechanisms enabling the system to safely interrupt its operation (fail-safe plans) in the presence of certain anomalies or when operation takes place outside certain predetermined boundaries. | SLICES will employ the technical and organizational measures necessary to provide protection to the users as well as secure the safety of the systems. |
| | | | Article 7 | AI is classified as high-risk accounting for: intended purpose, extended usage, nature of data processed, especially if special category, extended anonymity of actions and human involvement. | Based on the conditions in the Article, the AI model used for training and research purposes that boost innovation, should not be considered high-risk. However, SLICES will still implement all of the necessary measures to ensure compliance. |
| | | | Article 10 | Data sets used for training, validation, and testing must be pertinent, adequately representative, error-free, and full in light of their intended use. Providers of high-risk AI systems may, under appropriate safeguards for the fundamental rights and freedoms of natural persons, process special categories of personal data in | Users will be made aware if sensitive data is used for the training of the algorithm. Thus, they will have the necessary information to decide if they want to give their informed consent. If sensitive data is used, it will be in a GDPR-compliant manner. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | an exceptional manner if necessary to ensure bias detection and correction with regard to those systems. | |
| | | | Article 13 | It is imperative that high-risk AI systems are developed and constructed in a way that makes their functioning transparent enough for deployers to understand and make proper use of the system's output. A suitable level and kind of transparency must be maintained in order to achieve adherence to the applicable provider and employer requirements. | AI generated or tested through the SLICES-RI should avoid falling under the criteria for high-risk status, and should meet with this requirement regardless of the fact. |
| | | | Article 15(1) | High-risk AI systems must be created and developed with the goal of achieving the proper levels of cybersecurity, robustness, and accuracy. They must also function consistently in these areas over the course of their lifetime. | Although AI solutions that could be deployed in the SLICES-RI are unlikely to fall under the definition of high-risk AI, they will nevertheless ensure proper levels of cybersecurity, accuracy, and robustness, |
| | | | Article 60 | Any participants in real-world testing, may withdraw from the testing at any time by rescinding their informed consent and requesting the immediate and permanent deletion of their personal data, all without suffering any consequences or needing to give a reason. The legality or validity of already completed | After informing users of the requirements in Article 61, they will be provided with the possibility to withdraw their consent. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | activities will not be impacted by the withdrawal of the informed consent. | |
| | | | Article 61 | Before giving their consent, subjects should be informed of the nature and objectives of the testing, the conditions of the testing, their rights, arranging reversal of AI predictions, and the single identification number. | AI will encompass both support functions, such as integrating intelligent help bots like Rasa to help experimenters access and create experiments over the RI, and automatic code generation for running experiments over the RIs (*SLICES-SC Proposal*, 2020). This will be accomplished by collecting requirements from users in question forms and producing the relevant code for their experiment. Thus, SLICES will inform the users about the required information before they give their consent. |
| | | | Article 62(1)(b) | In order to meet the needs of SMEs, especially start-ups, users, innovators, and, where appropriate, local public authorities, member states shall plan particular awareness-raising and training initiatives on the execution of this Regulation; | SLICES will give students, researchers, and engineers access to remote experiments on equipment—which is frequently not available locally—as part of an innovative lifetime learning opportunity. Thus, the project will raise awareness about AI and train researchers on how to use it. |
| Commerce and consumer protection | Geo-Blocking Regulation (EU) 2018/302 | Preventing unjustified geo-blocking and other forms of discrimination based, directly or indirectly, on the customers' nationality, place | Art. 3 | Traders cannot refuse access to the interface based on location or nationality, and cannot redirect to region/nationality-specific versions of the interface, unless specifically provided why they should do so. | SLICES should prevent unjustified geo-blocking of access to the infrastructure |

| | | | | | |
|---|---|---|---|---|---|
| | | of residence or place of establishment | | | |
| | Digital Content Directive (EU) 2019/770 | Laying down common rules on certain requirements concerning contracts between traders and consumers for the supply of digital content or digital services | Art. 5, Art. 6, Art. 7, Art. 11, Art. 19 | Consumers should be provided with access to the content by the trader after concluding a contract. The access should meet subjective (as required by contract) and objective requirements for conformity and correct integration of content. The trader is liable for lack of conformities through the contract and minimum 2 years should be ensured for the consumer to invoke their rights. The trader can modify beyond maintenance requirements if the contract includes ongoing supply if: it is allowed by the contract, the consumer is informed and there are no extra costs; the modification is notified in advance. | When providing SLICES services to the public (exploitation phase), care should be taken to ensure compliance with quality-of-service requirements and consumer protection dispositions |

## Annex 2: Mapping with relevant standards

| SDO | Standard | Summary | Relevant Provision(s) or topics | Relation with SLICES |
|---|---|---|---|---|
| ISO | ISO/IEC 27001 Information Security Management | - Defining requirements for information security management systems. Facilitating cyber-resilience and risk management. | Information security management systems, risk assessment, risk treatment, information security policies, organization of information security, asset management, access control, cryptography, physical and environmental security, operations security, communications security, system acquisition, development and maintenance, supplier relationships, information security incident management, information security aspects of business continuity management, compliance. | SLICES shall ensure ICT and information security management, data integrity, confidentiality and resilience |
| | ISO/IEC 20000 IT Service Management | - Guidelines on what is expected from service providers in the context of their organisation.<br>- Lowering costs and increasing efficiency, optimising the provision of services. | IT service management, service delivery, relationship processes, resolution processes, control processes, and release management. | Efficient ICT service management is fundamental to a distributed research infrastructure like SLICES, particularly considering end-user/customer satisfaction requirements set by legal frameworks |
| | ISO/IEC 2382 Information Technology Vocabulary | - Providing guidance in defining and implementing processes to monitor and measure customer satisfaction. | Standard vocabulary for information technology, definitions of terms related to computing, data | As an ERIC, SLICES should align its vocabulary, definitions and terminology to ease usability regardless of language barriers |

| | | | | |
|---|---|---|---|---|
| | | | processing, and information systems. | |
| | ISO/IEC 30141 Internet of Things Reference Architecture | - Provides a standardized IoT Reference Architecture using a common vocabulary, reusable designs and industry best practices | Internet of Things (IoT) reference architecture, IoT system architecture, IoT functional view, IoT deployment and operational view. | This standard should be considered whenever integration of IoT-related services or infrastructures is considered in SLICES, so as to ease deployment and experimentation |
| | ISO/IEC 17788 Cloud Computing Overview | - Provides an overview of cloud computing along with a set of terms and definitions. It is a terminology foundation for cloud computing standards | Cloud computing overview, cloud service categories, cloud deployment models, key characteristics of cloud services. | As SLICES will make use of cloud technologies and develop a new one for automated RI as a Service (RIaaS), the services should follow the standards of this document. |
| | ISO/IEC 38500 IT Governance | - Provides guiding principles for directors of organizations (including owners, board members, directors, partners, senior executives, or similar) on the effective, efficient, and acceptable use of Information Technology (IT) within their organizations. | Corporate governance of information technology, principles for good governance, evaluation of IT performance. | As provided in Article 16 of the Statutes of Slices, the executive director will be in charge of representing the project and implementing the decisions of the supervisory board (*SLICES-SC Statutes*, 2024). As such, the executive director will follow the guidelines on how IoT is used and experimented within the project. |
| IEC | IEC 62443 Security for Industrial Automation and Control Systems | - Specifies in the form of best practices the procedures and conditions needed to install and maintain industrial automation and control systems that are electronically secure (IACS), | Security for industrial automation and control systems, cybersecurity risk assessment, system security requirements, and security management systems. | SLICES will establish an infrastructure that will provide a database for research purposes as well as space for experimentation. To achieve this, SLICES will make use of innovative digital technologies which will be protected through implementing the measures for cybersecurity set out in this standard. |

| | | | | |
|---|---|---|---|---|
| | IEC 62264 Enterprise-Control System Integration | - Explains the activities and interface material within the manufacturing operations management domain (Level 3), as well as the transactions that occur between Level 3 and Level 4. | Enterprise-control system integration, integration of manufacturing operations management and control systems, data models, and functional models. | SLICES will integrate data protection and cybersecurity measures. It will ensure also functional safety of the systems. |
| | IEC 61508 Functional Safety | - Establishes functional safety requirements for the lifetime of products and systems that are electrical, electronic, or programmable electronic (E/E/PE). It focuses on the components of an apparatus or system that carry out automated safety tasks. | Functional safety of electrical/electronic/programmable electronic systems, safety lifecycle, risk assessment, and safety integrity levels. | SLICES will achieve its goal in more than 10 research infrastructures (*SLICES-SC Proposal*, 2020). These infrastructures contain cutting-edge technologies such as IoT, Cloud and Wireless which have been created to account for the functional safety of the systems. |
| ITU | ITU-T Y.2060 Overview of the Internet of Things | - Provides an overview of the Internet of things (IoT). It clarifies the concept and scope of the IoT, identifies the fundamental characteristics and high-level requirements of the IoT and describes the IoT reference model. | Overview of the Internet of Things, IoT framework, IoT applications, IoT identification and addressing. | As the usage of IoT is crucial to the development of the project, this standard overview provides vital information on how to operate with IoT. |
| | ITU-T Y.3001 Future Networks | - Describes objectives and design goals for future networks (FNs). In order to differentiate FNs from existing networks, four objectives have been identified: service awareness, data awareness, environmental | Future networks, design goals, objectives for future networks, scalability, security, service universalization. | There will be connections made with the IEEE Future Networks Testbed Working Group's current standardisation initiatives, with the goal of standardising APIs and pressuring comparable platforms to adopt them globally (*SLICES-SC Proposal*, 2020). |

| | | | | |
|---|---|---|---|---|
| | | | awareness, and social and economic awareness. | | Thus, SLICES has ensured that the goals are aligned with the FN. |
| | ITU-T X.805 Security Architecture for Systems Providing End-to-End Communications | - | Defines the general security-related architectural elements that, when appropriately applied, can provide end-to-end network security. | Security architecture for end-to-end communication systems, security dimensions, security layers, security planes. | One of the platforms, which is used for the project, is LeonR&Do (*SLICES-SC Proposal*, 2020). The platform provides a testbed that operates with the end-to-end real network. It has been ensured that the platform's architecture is secure and safe on different levels. |
| | ITU-T Y.3501 Cloud Computing Framework | - | Provides a cloud computing framework by identifying high-level requirements for cloud computing. | Cloud computing framework, cloud service categories, cloud deployment models, key characteristics of cloud services. | SLICES will implement the relevant standards and frameworks which ensure that the cloud is regulatory compliant. |
| W3C | W3C WebRTC Standard | - | Defines a set of ECMAScript APIs in WebIDL to allow media and generic application data to be sent to and received from another browser or device implementing the appropriate set of real-time protocols | Real-time communication via browsers, audio and video communication, and data channels. | One of the goals of SLICES is to provide a network for researchers where they can build on their experiments through better infrastructure, databases, and communication. Thus, the exchange of input via audio and video channels will follow the ECMAScript. |
| | W3C Web of Things (WoT) | - | Counters the fragmentation of the IoT by using and extending existing, standardized Web technologies by providing standardized metadata and other re-usable technological building blocks | Web of Things, IoT device integration, semantic interoperability, web protocols for IoT. | The standard aligns with the goals of the ERIC for a common research infrastructure that centralizes IoT data. |

| | | | | |
|---|---|---|---|---|
| | W3C RDF Standard | - A standard model for data interchange on the Web. RDF has features that facilitate data merging even if the underlying schemas differ, and it specifically supports the evolution of schemas over time without requiring all the data consumers to be changed | Resource Description Framework, data interchange, metadata, data models. | The standard is a helpful tool for the interaction of data between the researchers in the infrastructure as it will ease data interoperability. |
| | W3C OWL Standard | - A Semantic Web language designed to represent rich and complex knowledge about things, groups of things, and relations between things. | Web Ontology Language, ontologies, semantic web, knowledge representation. | The language could be helpful for the description of the data. Moreover, to draw participants from a variety of backgrounds, all training activities will be created with multilingual support and cultural sensitivity in mind, which is why semantic web language is necessary for the project development (*SLICES-SC Proposal*, 2020). |
| ETSI | ETSI EN 303 645 Cyber Security for Consumer Internet of Things | - Support all parties involved in the development and manufacturing of consumer IoT with guidance on securing their products through high-level security and data protection provisions for consumer IoT devices that are connected to network infrastructure (such as the Internet or home network) and their interactions with associated services. | Cybersecurity for consumer IoT, security requirements, data protection, privacy. | SLICES will implement the necessary measures to provide data protection and cybersecurity. Some of these will be the protection by design and by default, anonymization, pseudonymization and erasing the data when it is no longer needed. |

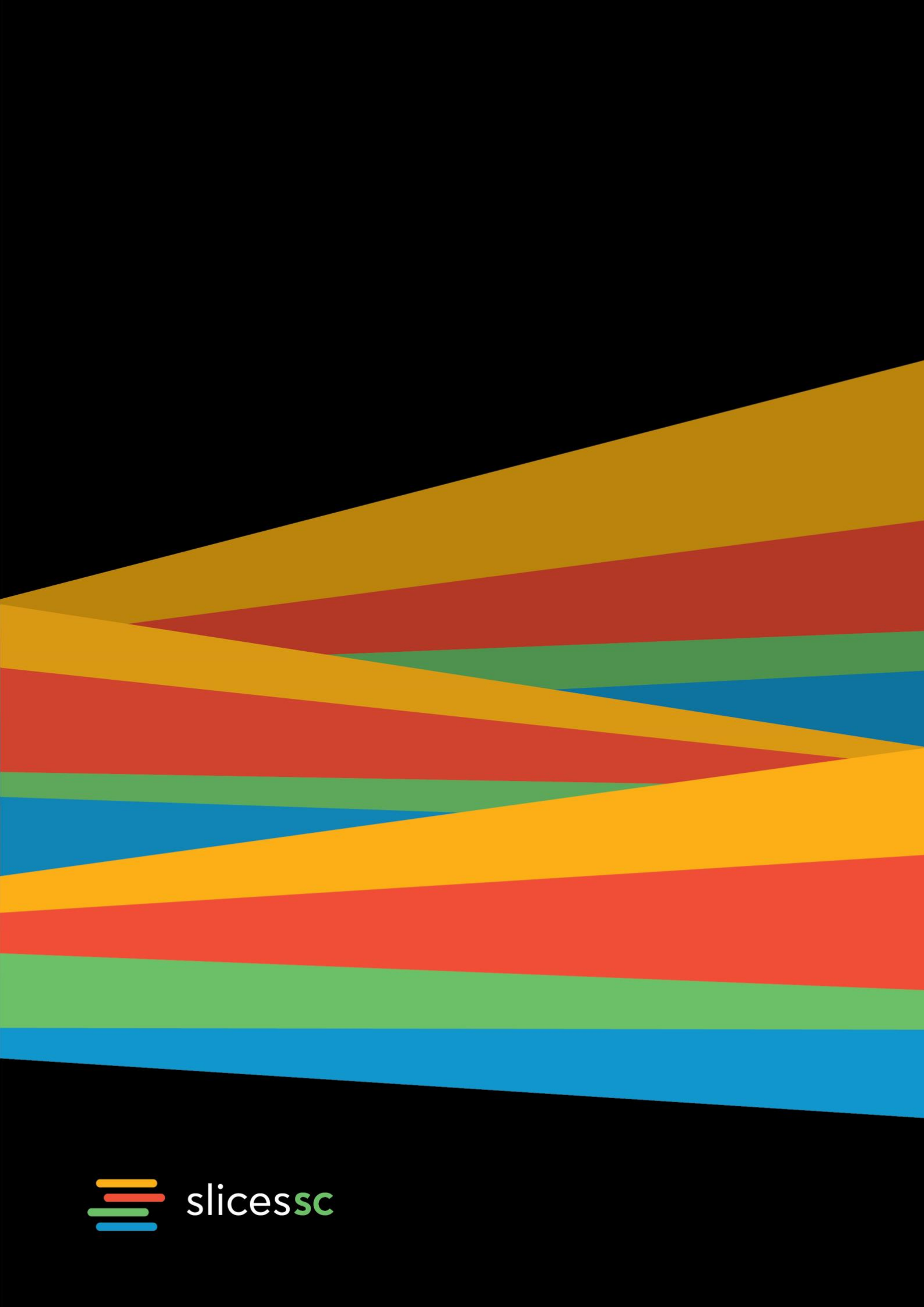
| | | | | |
|---|---|---|---|---|
| | ETSI Network Functions Virtualization (NFV) | - Virtualized network functions allow networks to be agile and capable of responding automatically to the needs of the traffic and services running over it. Achieved through key enabling technologies SDN (Software Defined Networking) and NFV (Network Functions Virtualisation) | Network Functions Virtualization, NFV architecture, NFV infrastructure, virtualized network functions. | A repository of ready-to-deploy experiments will be developed through the widespread use of Network Functions Virtualization (NFV), enabling users to fork, duplicate, and expand an experiment to suit their needs (*SLICES-SC Proposal*, 2020). The results will be shared in compliance with the FAIR principles. |
| CEN/CENELEC | CEN/CENELEC EN 50600 Data Centre Facilities and Infrastructure | - Operators and owners of data centres can: use a framework to standardise the processes and design of their data centres; ascertain the appropriate maturity level for their data centre;<br>find pertinent advice on possible areas for development and the expected benefits to support the need for the resources;<br>create a plan of action to transition to a higher degree of maturity. | Data center facilities, data center infrastructure, energy efficiency, data center management. | Data centres will be managed to account for EU policy objectives for sustainability and energy efficiency. These will be achieved not only externally through the experiments but also internally through how the centres are designed. |
| NIST | NIST Special Publication 800-53 | - Provides a catalogue of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other | Privacy, Personally Identifiable Information, Cybersecurity criteria | SLICES will follow the criteria for data protection and privacy, cybersecurity from the standard combined with the GDPR, the Privacy and Electronic Communications Directive, the Regulation on the free flow of non-personal data, the Data Governance |

| | | | | | |
|---|---|---|---|---|---|
| | | | organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks | | Act, and the European Data Act, as well as other standards from this table. |
| ECCP | Europrivacy – European Data Protection Seal | - | Approved by EDPB as European Data Protection Seal to assess and certify the compliance of all sorts of data processing under the GDPR and complementary national data protection regulations | Personal data protection, international data transfers, cybersecurity | SLICES may pursue certification with the Europrivacy certification (www.europrivacy.com), the EU Data Protection Seal, approved by the European Data Protection Board. |

## Annex 3: Industry Interview Questionnaire

The following are the suggested questions of the survey developed by SZTAKI for industry representatives' interviews:

1. Please rate the following Exploitable Assets (EAs) SLICES is providing. 1 meaning least valuable, 5 meaning most valuable for your company.
    a. Research Infrastructure
    b. Scientific Software Tools
    c. Scientific Hardware Tools
    d. Experimental Data
2. What are the exploitable results you plan to benefit from such an initiative like SLICES?
3. Can you think of any EA that does not fall under any category listed above, but would be beneficial for your company? Could you name those?
4. Would you be willing to pay for the use of SLICES related services in case it is important for you?
5. What is or would be the most valuable service for your company from SLICES RI?
6. Which SLICES Research Infrastructure would you like to access?
7. According to our current rules, we have cut-off dates for the SLICES Open Calls every 3-months. Our review process takes up to one month. Once the review is done you have a 3-month window to access the requested resources. Do you think it would be feasible to run projects with such scheduling?
8. Do you think you would need help to submit a proposal for one of the open calls?
9. Can you think of any obstacles that would prevent you from submitting a proposal for one of our Open Calls?
10. When it comes to training, what is your preferred method of learning? (F2F training(workshops), online training-real time, online training-on demand, MOOCs, etc.


slicessc