This deliverable is pending of approval by the European Commission.

Ref. Ares(2022)6452674 - 19/09/2022

HORIZON 2020
H2020 - INFRADEV-2019-3

D3.6 Data Protection Policies

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

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

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

www.slices-ds.eu

Executive Summary

SLICES aims at developing a pan-European network of research infrastructures, up to date with emerging and advanced technologies, that will support large-scale experiments and research. As such, SLICES is expected to receive, collect and process a significant amount of personal data, that either can lead to or actively lead to the identification of a natural person, regardless of whether said identification is direct or indirect. At the same time, it is evident that current legislative initiatives more and more shift the focus to the protection of such data within all frameworks, including for research purposes.

This Deliverable D3.6 presents in a brief yet explanatory manner the legal provisions that are applicable to personal data protection within the context of SLICES, as were further elaborated in Deliverable D1.3. The legislation included in the present deliverable remains relevant for the SLICES project throughout its lifecycle and shall be reviewed to consider any updates or amendments to the legal framework at each stage. Additionally, the crucial principle of data protection by design and by default is further explored.

This deliverable also expands on data protection implications for the research infrastructures, as envisioned during the design phase, as well as for experimenters choosing to conduct their experiments using the SLICES testbeds. Thus, having identified potential gaps and risks, the deliverable concludes with a number of organisational recommendations, best practices and policies that will ensure the creation and implementation of a robust data protection framework within the SLICES project.

Table of contents

1. Introduction and methodological approach

Deliverable D3.6 provides guidelines on how to implement and exploit the new Research Infrastructure in line with the principles of data protection by design. The data protection policies proposed in deliverable D3.6 permit to notably ensure that cross-border transfer is realised fully in compliance with the current regulation, in particular the GDPR. Directives such as the NIST and the ePrivacy are also to be taken into account in this deliverable. These policies should also prevent the generation of personal data from crossing various datasets provided by the different components of the future Research Infrastructure. Deliverable D3.6 proposes all necessary policies for data protection and data privacy, including the ethical aspect, to be implemented in the Research Infrastructure during the different phases of SLICES: design, development, and operation.

Methodological approach

The present deliverable builds upon previous deliverables on data management, data policies, as well as legal and ethical requirements that are relevant to the SLICES project. Firstly, it sets out a synopsis of **not only existing but anticipated legislation on a European and national level** regarding data protection, the use of data for research purposes, as well as copyright protection and open data requirements. The principle of **privacy by design and by default** is also expanded to clearly describe the notion and applicability for SLICES.

Subsequently, an analysis of the **implications for both experimenters, as well as the project itself** is conducted, describing the obligations and responsibilities imposed with regards to personal data protection and the protection of natural persons' rights and freedoms.

Furthermore, a series of **recommendations** on an organisational structure level, as well as in the context of designing the data protection policy are made, in order to ensure data protection compliance for the SLICES project on all levels. Finally, future required actions for SLICES-SC and SLICES-PP are described, for the purpose of further evolving the project.

Legal Requirements Analysis

In order to identify and determine the essential provisions for the SLICES project, current and intended legislation has been examined, starting from the main legal instrument – the General Data Protection Regulation (GDPR) – as well as more recent legislative proposals on data protection online, the protection of databases and public held data, the use of data in research, copyright and open science requirements. At the same time, the relevant national provisions are briefly mentioned, explaining whether the GDPR is applied within the territory of a discussed country, on what basis it is applied, and whether the respective country's national legislation includes specialised provisions for the use of personal data for research purposes.

Following the detailed analysis already carried out in previous deliverables, the present deliverable includes a table of each legislative instrument, presenting a summary of the rationale and goals of the legal text, its central idea, certain principal provisions describing the requirements laid out by the law, as well as the significance of the legislation for the SLICES project. As a result, the tables form a useful tool to be reminded of the content and main ideas of each legal text.

In addition, the central personal data protection principle of privacy by design and by default is further analysed explaining its definition, legal basis, as well as its implications for researchers involved with SLICES.

2. Data Protection Legal Requirements and Liability for SLICES

2.1. GDPR[1]

Rationale	The establishment of a comprehensive framework protecting **personal data and the right to privacy in the digital era.**
Focal points	Establishing a set of **principles for data collection and data processing**, namely: **a.** Lawfulness, **b.** Fairness, **c.** Purpose, storage and time limitation, **d.** Data minimisation, **e.** Data protection by default and by design, **f.** Accuracy, integrity and confidentiality of data, and **g.** Transparency and accountability.
Selected specific provisions	• Data collection and processing must be based on a **legal basis as defined in the GDPR.** • **Consent** is required for the processing of special categories of data and further processing. • Data subjects have a series of **rights** that must be respected at all times. • A **Data Protection Officer (DPO)** shall be assigned based on the controllers' and/or processors' activities. • A **Data Protection Impact Assessment (DPIA)** shall be performed when an activity results in high risk for the data subjects' rights and freedoms.
Importance for SLICES	The GDPR is crucial for every entity that may collect, process or store personal data referring to an identifiable natural person. SLICES is also bound by the relevant data protection obligations when its activity involves personal data.

2.2. EPrivacy

2.2.1. EPrivacy Directive[2]

Rationale	The completion of the **electronic communications data protection and privacy** framework.
Focal points	**i.** Regulation of privacy rights in electronic communications, **ii.** Regulation of cookies, **iii.** Traffic data shall also be confidential.

[1] European Council European Parliament, 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)', Pub. L. No. 32016R0679, 119 OJ L (2016), http://data.europa.eu/eli/reg/2016/679/oj/eng, [Last accessed 31 August 2022].

[2] European Parliament, 'Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications)', 6 December 2002, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058, [Last accessed 31 August 2022].

Selected specific provisions	• The nature of such services is highly sensitive and requires additional attention. • The directive applies to all providers of such services operating in the EU territory. • Appropriate **technical and organisational security measures**, in accordance with the **state-of-the-art** shall be adopted. • Data subjects must be informed about **breaches** of their personal data. • Data subjects' **consent** must be acquired for any tracking activities, such as cookies. • **Traffic data and location data** are considered personal data and are subject to data protection principles. • **Transmission and storage** of data in public directories must abide by data protection provisions.
Importance for SLICES	The ePrivacy Directive provisions are relevant for SLICES' online activity until the Directive is repealed and replaced by the ePrivacy Regulation.

2.2.2. EPrivacy Regulation[3]

Rationale	The expansion of the established framework and the **modernisation of the ePrivacy directive**, in accordance with the GDPR.
Focal points	**i.** More players of electronic communications services, **ii.** A set of stronger yet simpler rules on data protection, **iii.** The expansion of protected activities to include additional content and metadata, **iv.** Protection against spam, **v.** More effective enforcement, **vi.** New business opportunities.
Selected specific provisions	• **Metadata** has the same potential as the content of electronic communications itself to reveal highly sensitive information about the users. • The **principles of proportionality and necessity** must be respected at all times during the processing of original data and metadata. • Electronic communications data may be processed for the purposes of transmission of communication and to restore security or to fix technical errors. • Metadata may be processed for the purposes of maintaining a high quality of services, billing and interconnecting payments, detection and ceasure of fraudulent and/or abusive actions. • **Consent** shall be sought for the processing of electronic communication data and metadata. • Once the purposes have been met, the above data shall be erased or anonymised. • Strict conditions shall apply for the **processing and storage of information related to the end-users' equipment**. • **Data subjects' rights** are expanded to assist them in acquiring control of their data. • GDPR provisions on remedies, compensation, and liability apply.

[3] European Commission, 'Proposal for Regulation on Privacy and Electronic Communication', Pub. L. No. 2017/003 (COD) (2017).

Importance for SLICES	The provisions of the ePrivacy Regulation are relevant for the proper operation of the SLICES website and could be of relevance to the expected services of the SLICES platforms.

2.3. Data Act4

Rationale	The improvement of the framework regarding **data use and accessibility**, to match the goals set for the EU's internal market.
Focal points	**a.** Enabling users of connected devices to gain access to data generated by them and share them as desired, without this meaning that manufacturers will be bearing additional costs or that the data generated by them will be used in direct competition with them, **b.** Rebalancing the negotiation power of Small and Medium Entreprises (SMEs) during their contractual relationships with stronger players, **c.** Enabling users to switch between different cloud data-processing service providers while preventing unlawful data transfers. **d.** Reviewing the Database Directive's provisions on data derived by Internet-of-Things (IoT) devices to facilitate their use.
Selected specific provisions	• A clearer set of **data-sharing guidelines** between businesses and consumers and among businesses is defined. • The users must be provided in advance a **minimum of information** on the data that the product or service will generate, collect and process, who will have access to it and how users can access it, share it and defend their rights. • Third parties receiving shared data must process them in accordance with the users' wishes and data protection principles. • Data sharing is performed in in a **fair, reasonable and non-discriminatory manner** and is subject to a **reasonable compensation** where required. • **Interoperability** of data is a principal obligation of the operators of data spaces.
Importance for SLICES	The Data Act provisions shall be considered for the SLICES project, taking into consideration that it is intended to resume the position of a data holder and data recipient, possibly providing data processing services. Interoperability is also a central ethical obligation for researchers within the open science framework.

2.4. Data Governance Act5

Rationale	The establishment of a robust framework for **data sharing and use for research purposes.**
Focal points	Enabling the re-use of data held by public sector bodies, which are protected on the grounds of commercial and statistical confidentiality, protection of intellectual property rights or the protection of personal data.

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

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

Selected specific provisions	• Public sector bodies holding data may set a series of **criteria for the re-use** for research purposes, which shall be **non-discriminatory, proportionate and objectively justified**, focusing on **data protection, confidentiality, encryption, and security of data, as well as any intellectual property rights**. Such re-use may be subject to a reasonable fee. • Agreements and policies granting **exclusive rights** or restricting availability of data for re-use are allowed under certain conditions. • A series of **prerequisites for data sharing** is provided, which do not apply to non-profit entities who solely focus on collecting data for reasons of general interest that are later made available on the basis of data altruism. • A **data altruism organisation registry** shall be established.
Importance for SLICES	The Data Act provisions shall be considered for the SLICES project, taking into account that it is intended to resume the position of a data holder and data recipient, possibly providing data processing services. Interoperability is also a central ethical obligation for researchers within the open science framework.

2.5. Digital Services Act[6]

Rationale	The **regulation of platforms offering intermediary digital services** in the Union's market.
Focal points	Establishing new rules on liability of providers of intermediary digital services on: - Mere conduit - Caching - Hosting
Selected specific provisions	• There is **no general obligation to monitor the information transmitted or stored** through the intermediary service providers. • If **illegal content** is located, it shall be removed as soon as possible. • Service providers shall abide by **due diligence and transparency** obligations. • Service providers shall establish a **single point of contact** for direct communication and adequate procedures to allow notification of illegal content. • Large online platforms and very large online platforms are subject to stricter requirements of protection of users and risks identification.
Importance for SLICES	The SLICES project shall consider the provisions of the Data Service Act since the testbeds shall be providing intermediary digital services.

2.6. Database Directive[7]

Rationale	The **legal protection of databases**, whether physical or electronic.
Focal points	Establishing a **dual system of protection**: ○ Copyright protection of the database itself ○ A *sui generis* intellectual property right on the content of the database

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

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

Selected specific provisions	• The **database itself** is protected when it forms the author's own intellectual creation, either due to selection or arrangement of content. • The author is identified with the **rightsholder of copyright** and exclusively assumes a series of rights over the database. • **Exceptions to the exclusive rights** may be provided, among others, on the basis of scientific research. • Rights over the **content of the database** are freely transferred, assigned, or granted under a contractual license. • Creators of database content are granted protection under the condition that they are nationals of an EU Member State or they have their habitual residence or establishment in the EU, unless an agreement states otherwise.
Importance for SLICES	Databases in scientific research are extremely relevant for the SLICES project, thus the requirements of access and intellectual property rights related to them must be taken into account.

2.7. Network and Information Security Directive

2.7.1. NIS1 (current version)

The Directive 2016/1148[8] on security of network and information systems[9] (NIS Directive) is the first piece of cybersecurity legislation passed by the European Union (EU) and provides legal measures to **boost the overall level of cybersecurity in the EU**. The Directive was adopted in August 2016 with an aim to harmonise cybersecurity capabilities in all EU Member States and to ensure that **exchanges of information and cooperation** initiatives are efficient, including at a cross-border level. The NIS directive sets a range of **network and information security requirements** that apply to **operators of essential services and digital services providers**.

The NIS Directive requires each EU Member State to put together a list of organisations within those sectors that they consider to be essential service providers and adopt a national strategy on the security of network and information systems defining strategic objectives and appropriate policy and regulatory measures.

The table provides information and reference to the **Member States' national implementation laws or amended existing legislation** following the adoption of the NIS directive. Moreover, the national additional obligations or requirements in relation to Operators of Essential Services[10] are listed below.

[8] European Parliament and European Council, 'Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union', 19 July 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC, [Last accessed 31 August 2022].

[9] Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L1148, [Last accessed 13 June 2022].

[10] See https://www.digitaleurope.org/resources/nis-implementation-tracker/, [Last accessed 15 June 2022].

Country	Member States' National Implementation Law. The national specification in relation to Operators of Essential Services (OES).
Austria	Federal Act for a High Common Level of Security of Network and Information Systems
	OES summary: the scope for Operators of Essential Services is the same laid down in the NIS Directive, with the inclusion of public administration.
Belgium	In progress
Bulgaria	Cyber Security Act (94/2018)
	OES Summary: The list of OES is the same as listed in the NIS Directive alongside the scope and OES requirements.
Croatia	In progress
Cyprus	The Security of Network and Information Systems Law of 2018
	OES Summary: Additional industries that are considered OESs include electronic communications, wastewater, food, government and national security/ emergency services and environmental.
Czech Republic	Cyber Security Act
	OES Summary: The Czech legislator has specified the criteria to identify operators of the essential services here
Denmark	the Danish Requirements for Security of Network and Information Systems within the Health sector, ACT (no. 440/2018) Executive Order (no. 458/2018) Executive Order (no. 459/2018)
	OES Summary: The Danish Government has transposed 12 new bills that are sector-focused. Each of the acts defines operators of essential services in each sector.
Estonia	Cyber Security Act
	OES Summary: Under the Estonian implementation legislation, Operators of Essential Services also include electronic communication service providers, public broadcasting, providers of digital identification and digital signing service, and district heating service providers.
Finland	The obligations of NIS directive are laid down in legislation within each sector, and the supervisory authorities in these sectors monitor their compliance.
	OES Summary: With the Finnish national legislation industries such as online marketplaces, search engine, cloud providers and other digital infrastructures are considered OES.
France	Decree No. 2018-384

	OES Summary: Industries that are considered OES within the French legislation include industries involved in the civil activities of the State, judicial activities, military activities of the State, food, electronic, audio-visual and information communication, space and research, and finance industries.
Germany	Implementation Act (Federal Law Gazette, BGBI. I 2017 of 29 June 2017) amending the Act on the Federal Office for Information Security, Atomic Energy Act, Energy Industry Act, Social Insurance Code V and the Telecommunications Act
	OES Summary: The German regulation determines the facilities that qualify as critical infrastructure in Germany Ordinance of Critical Infrastructure under the Act on the Federal Office for Information Security
Greece	In Progress
Hungary	Act 134 of 2017 Government Decree 394/2017 (XII. 13)
	OES Summary: OES within the Hungarian national legislation are the same as described in the NIS Directive.
Ireland	Statutory Instrument No. 360 of 2018
	OES Summary: Sectors that revolve around energy, transport, banking, financial market infrastructure, health, water, and digital infrastructure are all considered OES.
Italy	Legislative Decree 65/2018
	No additional changes from the NIS Directive.
Latvia	IT Security Law
	OES Summary: The OES Scope is the same as indicated within the NIS Directive, however, both banking and financial market infrastructure sectors have sector specific legislation and requirements.
Lithuania	**In progress**
Luxembourg	**In progress**
Malta	**In progress**
Netherlands	Network and Information Systems Security Act
	OES Summary: The requirements and scope of OES is the same as the NIS Directive, however, with the exclusions of health sector.
Poland	Act of 5 July 2018 on the National Cyber Security System
	OES Summary: According to the Polish national legislation, OES are the same as indicated in the NIS Directive with the inclusion of the heating and mining sub-sectors.
Portugal	The legal regime of Cyberspace Security – Law No. 46/ 2018 of August 13

	OES Summary: Public administration and critical infrastructures fall within the jurisdictional oversight of the cybersecurity authority; however, they are not subject to the OES requirements.
Romania	Ensuring high level of security of information networks and systems
	OES Summary: No divergence from NIS Directive obligations and scope for OES.
Slovakia	Act of January 30, 2018 on Cybersecurity and on Amendments and Supplements to certain Acts.
	OES Summary: OES listed within the Slovakian legislation are the same as described in the NIS Directive, with the addition of pharmaceutical/ chemical industry, public administration, electronic communication, postal service.
Slovenia	Act on Information Security (Official Gazette of the RS, No. 30/18)
	OES Summary: The same scope and requirements listed in the NIS Directive apply to the national legislation, with the addition of environmental protection industries.
Spain	Royal Decree-Law 12/2018, September 7, on security of networks and information systems – date of application20/09/2018
	OES Summary: No changes from NIS Directive requirements.
Sweden	Law on information security for socially important and digital services
	OES Summary: No changes from NIS Directive requirements.

2.7.2. NIS2 (upcoming revision)[11]

Rationale	The adaptation of the **cybersecurity management** to the evolution of technology and modern cyberthreats.
Focal points	**Expanding the scope** of application to include important and essential entities, thus excluding only micro and small enterprises.
Selected specific provisions	• The Directive builds on the existing framework. • **Cybersecurity tools and relevant measures** shall sustain the general **availability and integrity** of the public core of the internet. • The existing Computer security incident response teams (CSIRTs) are additionally obliged to **disclose vulnerabilities** to the ENISA **in a coordinated way**. • Specific authorities shall be assigned with the duty to **manage large-scale incidents and crises.** • A **peer-review system** for assessing cybersecurity policies shall be established.
Importance for SLICES	Given the importance of the projects carried out via the SLICES infrastructure, as well as its Internet of Things and interconnection capacities, SLICES would be vulnerable to cyberattacks if there was no adequate cybersecurity framework. It is essential that

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

	obligations under the NIS directives are understood and taken into account when designing and updating the cybersecurity framework.

2.8. AI Act[12]

Rationale	To lay a common legal framework for development, marketing, and the use of AI products and services in the EU
Focal points	**1.** Ensuring AI systems' safety and compliance with existing law on fundamental rights and EU values, **2.** Enhancing legal certainty to foster investments and innovation initiatives in AI, **3.** Improving governance and effective enforcement of existing fundamental rights legislation and safety requirements, and **4.** Gathering lawful, safe and trustworthy AI applications under a single market and preventing market fragmentation.
Selected specific provisions	• The Regulation shall encompass **machine learning approaches, logic and knowledge-based approaches, as well as statistical approaches, Bayesian estimation, and search and optimisation methods**. • **AI-related risk** is divided into the following: ➢ **Unacceptable risk,** providing a clear threat to the safety, livelihoods, and rights of data subjects, including but not limited to generalised profiling by public bodies and systems that encourage dangerous behaviour. ➢ **High-risk by nature**, due to its relevance to vital sectors of everyday life, such as employment, critical infrastructure, access to public services, etc., they are subject to a risk management system, development of appropriate data governance, and maintenance of technical documentation. Such systems shall, thus, be subject to a conformity assessment prior to circulation, along with a written EU declaration of conformity. ➢ **Minimal risk**, for which a code of conduct is envisioned.
Importance for SLICES	Since SLICES shall employ AI methods, it is essential that it abides by not only the provided ethical guidelines, but also the relevant legislation.

2.9. Open Data and Public Sector Information Directive[13]

Rationale	The **reinforcement of open data practices**, in particular in the public sector, so publicly held data can be re-used.
Focal points	Making **available public sector data in free and open formats**, so that it can be further utilised for research purposes and to improve the internal market, impacting society and economy.
Selected specific provisions	• **Publicly held data and certain research data** may be re-used for research purposes, unless they are related to competition, intellectual property rights,

[12] Council of the European Union, 'Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts-Presidency Compromise Text', 29 November 2021, 2021/0106 (COD).

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

	sensitive national security data, personal data rights or are held by cultural establishments or research organisations. • A **procedure for the re-use** shall be followed. • Access to the data shall be **free of charge** (with the exception of technical costs), **non-discriminatory and shall not grant exclusive rights** unless required to protect the public interest. • Access to **high-value datasets** shall be free of charge, machine readable, provided by APIs and as bulk download where relevant. • Member States shall adopt **open access policies,** in accordance with the open by default and FAIR principles, respecting intellectual property rights, personal data, security and legitimate interests.
Importance for SLICES	SLICES provides research infrastructure to which data is crucial. Open access and open science principles are vital for the realisation of the project.

2.10. Copyright Directive[14]

Rationale	The **harmonisation of the legal framework regarding copyright** in the context of the Union's Digital Single Market.
Focal points	Balancing the rights derived from copyright and open science requirements to foster scientific research, experimentation and innovation, providing a number of relevant exceptions.
Selected specific provisions	• **Exclusive reproductive rights** are maintained, **unless an exception** is based on text and data mining for the purposes of **scientific research**, teaching activities and the preservation of cultural heritage. • **Licensing** shall be improved while ensuring wide access to content in a number of cases, including when protected content is used by online content-sharing service providers. • **Appropriate and proportionate remuneration** is provided for the use of protected authors' and performers' content. • Creators maintain the **right to revoke any licenses or authorisations**.
Importance for SLICES	SLICES research infrastructures shall provide to experimenters the opportunity to freely conduct their experiments. Nonetheless, users are at all times required to respect copyright and intellectual property rights.

2.11. National Laws pertaining scientific use of data

European Union

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

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

research purpose is processed, in accordance with the **principle of data minimisation** outlined in Article 5 (c) of the GDPR.

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

Since Recital 26 asserts that **pseudonymised data is considered personal data** as long as it can be attributed to a natural person in combination with additional information, the Regulation also applies to pseudonymised data.

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

Country	GDPR application	National provisions on data protection and scientific research
Austria	Yes, EU Member State	Yes, Federal Act concerning the Protection of Personal Data
Belgium	Yes, EU Member State	Yes, Belgian Act of 30 July 2018 on the Protection of Natural Persons with regard to the Processing of Personal Data
Bulgaria	Yes, EU Member State	No additional provisions
Croatia	Yes, EU Member State	No additional provisions
Cyprus	Yes, EU Member State	Yes, Cypriot Law 125(I) of 2018 on The Protection of Natural Persons with regards to the Processing of Personal Data and for the Free Movement of Such Data
Czech Republic	Yes, EU Member State	Yes, Czech Act No. 110/2019 Coll. On Personal Data Processing
Denmark	Yes, EU Member State	Yes, Data Protection Act of Denmark
Estonia	Yes, EU Member State	Yes, Estonian Personal Data Protection Act 2018
Finland	Yes, EU Member State	Yes, Data Protection Act of Finland
France	Yes, EU Member State	Yes, Law n° 2018-493 of 20 June 2018 and Law n° 78-17 of 6 January 1978 for health data
Germany	Yes, EU Member State	Yes, German Federal Data Protection Act

Greece	Yes, EU Member State	Yes, Greek Law 4624/2019, implementing Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons concerning the processing of personal data, and transposition of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016, and other provisions
Hungary	Yes, EU Member State	Yes, Hungarian Act CXII of 2011 on the Right of Informational Self- Determination and on Freedom of Information
Iceland	Yes, Decision No. 154/2018 of the EEA Joint Committee	Yes, Icelandic Act 90/2018 on Privacy and Processing of Personal Data
Ireland	Yes, EU Member State	Yes, Irish Data Protection Act 2018
Italy	Yes, EU Member State	Yes, Italian Legislative decree no. 196 of 30 June 2003
Latvia	Yes, EU Member State	No additional provisions
Liechtenstein	Yes, Decision No. 154/2018 of the EEA Joint Committee	Yes, Liechtenstein Data Protection Act of 4 October 2018 and Data Protection Ordinance of 11 December 2018
Lithuania	Yes, EU Member State	No additional provisions
Luxembourg	Yes, EU Member State	Yes, Luxembourg Act of 1 August 2018 on the Organisation of the National Commission for Data Protection and Implementing the GDPR
Malta	Yes, EU Member State	Yes, Maltese CAP 586
Netherlands	Yes, EU Member State	Yes, Dutch GDPR Implementation Act
Norway	Yes, Decision No. 154/2018 of the EEA Joint Committee	Yes, Norwegian Personal Data Act of 15 June 2018 on special categories of data and criminal convictions data
Poland	Yes, EU Member State	Yes, Polish Personal Data Protection Act of 10 May 2018
Portugal	Yes, EU Member State	Yes, Portuguese Law no. 58/2019
Romania	Yes, EU Member State	Yes, Romanian Law No. 190/2018 Implementing the General Data Protection Regulation
Slovakia	Yes, EU Member State	No additional provisions

Slovenia	Yes, EU Member State	Yes, Slovenian Personal Data Protection Act
Spain	Yes, EU Member State	Yes, Spanish Organic Law 2/2018 on Data Protection and Guarantee of Digital Rights
Sweden	Yes, EU Member State	Yes, Swedish Act containing Supplementary Provisions to the EU General Data Protection Regulation (SFS 2018:218)
Switzerland	Yes, Decision No. 154/2018 of the EEA Joint Committee	Yes, Swiss Federal Act on Data Protection
UK	Not after 31 December 2020	Yes, UK General Data Protection Regulation

A detailed description of the above-mentioned national provisions is available at deliverable SLICES-DS 1.3, Annex I.

3. Data Protection by Design and by Default

3.1. Legal Basis and definition

The development of projects such as digital infrastructure which involves the processing of personal data requires the implementation of data protection measures. The GDPR provides for two crucial concepts for future project planning: data protection by design and data protection by default[15].

Article 25 (1) of the GDPR requires to implement both at the time of the means of processing and at the time of the processing itself, **appropriate technical and organisational measures** that are designed to implement data protection principles and to integrate **necessary safeguards** into the processing in order to meet the requirements and protect the rights and freedoms of the individuals.

The term 'measures' can be understood in a broad sense, meaning **any method or means that a data controller may employ in the processing of personal data.** Such measures must be appropriate, suitable for achieving the intended purpose, and effectively implement the protection of personal data, reducing the risks of violation of the rights and freedoms of data subjects[16].

[15] Data Protection Commission of Ireland https://www.dataprotection.ie/en/organisations/know-your-obligations/data-protection-design-and-default [Last accessed 16 June 2022]

[16] Francesco Cucci, 'Data Protection by Design e by Default: Le Implicazioni Operative e Organizzative Sulle Aziende', n.d., https://www.cybersecurity360.it/legal/privacy-dati-personali/data-protection-by-design-e-by-default-le-implicazioni-operative-e-organizzative-sulle-aziende/. [Last accessed 16 June 2022]

On the other hand, **data protection by default** in accordance with article 25 (2) of the GDPR requires to implement appropriate technical and organisational measures for ensuring that, by default, **only personal data, which is necessary for each specific purpose of the processing are processed**[17].

3.2. Definition

On one hand, **data protection by design** is the approach that ensures data protection **is considered early during the design phase** of any system, service, product and process and is **maintained throughout their lifecycle**. This entails that appropriate technical and organisational measures are put in place from the onset of the project, as well as adequate safeguards to protect data subjects' rights.

Data protection by default requires that **only data which is necessary for the specific purpose** set are collected and processed, thus providing a **direct link to the principles of data minimisation and purpose limitation**. This means that prior to the processing, it is important to not only lay out the exact purposes for which data shall be collected and processed, but also to inform the data subject of these decisions.

Merging the two notions, the concept of privacy by design and by default results in the obligation to develop proper solutions that will ensure data protection from the start of the project and throughout its lifecycle, collecting data only when required to meet the specific purposes defined, while respecting the principles of data minimisation and purpose minimisation.

3.3. Applicability

The GDPR, specifically in Article 25 (1), provides some elements that must be taken into account when determining the measures of a specific processing operation. This list includes the following elements[18]:

State of the art: it means that when determining appropriate technical and organisational measures the data controller shall take into consideration the current progress of technology that is available in the market. The requirement is to have knowledge of, and stay up to date on technological advances; how technology can present data protection risks or opportunities to the processing operation; and how to implement and update the measures and safeguards that secure effective implementation of the principles and rights of data subjects taking into account the evolving technological landscape. This criterion applies also to organisational measures. A lack of appropriate organisational measures can lower or even completely undermine the effectiveness of a chosen technology.

Cost of implementation: the cost of implementation is a factor to be considered in implementing data protection by design. It may be taken into account when choosing and applying appropriate technical and organisational measures and necessary safeguards. The cost refers to resources in general, including time and human resources.

[17] Information Commissioner's Office: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/ [Last accessed 16 June 2022]

[18] Guidelines 4/2019 on Article 25 Data Protection by Design and by Default of the EDPB: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2019/guidelines-42019-article-25-data-protection_en [Last accessed 17 June 2022]

Nature, scope, context, and purpose of processing: the concept of nature can be understood as the inherent characteristics of the processing. The scope refers to the size and range of the processing. The context relates to the circumstances of the processing, which may influence the expectations of the individual, while the purpose pertains to the aims of the processing.

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.

4. Implications for the Experimenters

It has been established that, when conducting an experiment, there is an **ethical and legal obligation** imposed on researchers to bear in mind and protect the **privacy and confidentiality of any personal data involved in their research project.** Taking into consideration that the testbeds intended to be developed via the SLICES project shall permit the performance of experiments and research projects by its users, data protection requirements shall apply to the experimenters utilising the platform as well.

The first step towards the establishment of a sound data protection framework that shall be applicable to the testbeds' experimenters is the **determination of whether experimenters shall be allowed to use personal data** in their experiments.

In the affirmative, experimenters[19] shall be **required to abide by a number of policies** referring to the following matters:

- **i)** Consent of the data subjects whose data shall be used
- **ii)** A clear definition of original and secondary use of data, followed by concise rules in sectors such as:
  - a. Purpose and lawfulness of processing
- **iii)** Transparency throughout the entire experiment, and in particular regarding the following:
  - a. Use of data
  - b. Recipients of data
  - c. Access rights
- **iv)** Pseudonymisation and anonymisation techniques utilised
- **v)** Processing of sensitive data
- **vi)** Data subjects' rights
- **vii)** Data quality
- **viii)** Data retention period
- **ix)** Deletion and archiving of data
- **x)** Data transfers
- **xi)** Publication of results

[19] Under this assumption, experimenters would become data controllers for any personal data processed in the course of their experiment.

In case experimenters are not to use the platform for experiments involving personal data that can be linked to an identifiable person, they shall be in the position to **guarantee that no such data shall be used while abiding by the general data protection principles**.

Where **anonymised data** shall be used, they shall bear the responsibility of ensuring that any **de-anonymisation tools are kept securely, independently from the testbeds**. At the same time, they shall be solely liable in case they or their affiliated organisation violates the relevant personal data protection requirements.

In all cases, experimenters need to be **provided, upon registration, with a complete set of information regarding personal data**, what constitutes personal data, the precise categories of sensitive data, as well as their obligations and rights regarding data subjects' personal 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.

5. Implications for the RI (SLICES)

5.1. Contractual and User Access Implications

Within the framework developed by the GDPR, it is essential that each party involved in data collection, processing, transfer or storage has been clearly **allocated a specific set of obligations, responsibilities and rights**. Such allocation of function shall be based on **contractually established relationships** within the SLICES project. In particular, in the context of SLICES, **Joint Controllership Agreements (JCA)** shall be signed, transparently defining the role of each of the multiple partners acting as data controllers.

Accordingly, a **Data Processing Agreement (DPA)**[20] shall be signed with the respective data processors, laying out distinct **instructions on the following:**

- The subject matter of the processing, as well as the categories of data involved,
- The nature and purpose of the processing,
- The duration of the processing and provisions on how data is handled after the expiry of the processing period,
- Confidentiality requirements for staff members,
- Security measures in place,
- Technical and organisational measures in place to protect data subjects' rights,
- The obligations and rights of each party.

SLICES shall solely appoint **processors and third-party providers** (for storage and similar services) offering **sufficient guarantees of compliance with data protection requirements**, taking into consideration **certifications, seals and marks of conformity**. Within this context, SLICES processors

[20] Details concerning the implementation of the DPA, Joint Controllership Agreement and/or potential need for a standardized data sharing agreement should be defined once the SLICES project reaches a higher level of maturity.

shall aim at having their data processing operations certified as data protection compliant by respected certification schemes, recognised by the EU.

Nonetheless, data protection legislation has impacted organisation-user relationships as well. Specifically for SLICES, it is essential that the **relationship between experimenters and the testbeds is duly defined,** in order to ensure both parties agree on and comprehend the nature of the activities carried out. In the case of experimenters, such contractual relationships are two-fold, depending on the nature of the decided SLICES possibilities, namely:

1) An **agreement on the use of the platforms**, that shall involve all experimenters looking include provisions on which personal data on the experimenters shall be collected and processed, how it shall be used and for how long, who shall have access to it, the security, technical and organisational measures in place, the proper use of the testbeds, the services that shall be utilised by the experimenter and under which conditions, as well as each party's rights and obligations.
2) The second contractual relationship established depends on the SLICES choice or lack thereof to provide the opportunity for **experimenters to use personal data** in the experiments they intend to perform using the testbeds. In the affirmative, SLICES testbeds shall assume the role of a data processor, with the experimenter as the data controller and, therefore, a DPA, as described above, shall be required. In the case that will not be allowed, the agreement signed with the experimenters shall explicitly exclude the possibility, requesting that the experimenters assume the responsibility of either completely excluding personal data or having it anonymised.

Similarly, **access to the testbeds** needs to be further specified, in order to not only ensure that the experimenters' personal data is protected, but also to secure the content of the experiments and their intellectual property rights. Such access shall be protected by an authentication of user procedure that shall require a username and password, as well as an additional authorisation step. Other parties shall be able to view a limited amount of information on the experimenter, such as the username.

If **multiple users** are allowed to work on the same experiment, it is necessary that backups and log records are securely maintained for verification purposes. This will not only aid in verifying the person making changes, but it will also protect the data from alteration, destruction or loss due to technical errors or unauthorised access. Moreover, an **allocation of roles** will be useful to define each party's rights within the same experiment, such as main experimenter and contributors, to ensure that the external hierarchy among experimenters is respected. Finally, it should be possible for **experimenters to authorise access** to an experiment through the use of an additional pin code, to restrict access for a number of reasons, including confidentiality or copyright protection.

5.2. Personal Data Processing Mapping

Data mapping is a crucial component of the GDPR, as the **preparatory step to fulfil all data protection requirements**. As such, personal data processing mapping thoroughly describes:

1) The **categories of data** that are collected and processed, including whether they involve sensitive data,
2) The **sources of personal data**,
3) The processing's **purposes and lawfulness**,
4) The **intended usage** of data,

5) The location where data is **stored**, as well as the **storage period and access requirements**,
6) The **route of the data** within the organisation, as well as any **data transfers and third-party recipients.**

Apart from the self-explanatory benefit of compliance with the GDPR requirements, in particular **Article 30** requiring recording of processing activities, data mapping additionally can contribute to **identifying privacy risks, planning a more efficient security network, as well as responding to data subjects' requests** in accordance with their rights to access, transfer, restrict, correct or delete their data. The data processing mapping shall also serve as a **demonstrator of privacy by design** within the project, while it shall also aid in performing an adequate DPIA.

Data mapping can be performed **either manually or using a software tool** in that direction, with a flow chart appearing as the most easily comprehensible and, thus, effective visual representation form. The GDPR does not specify any preferred format for the data mapping, as data mapping itself is not explicitly mentioned within its text but is viewed as a **best practice for compliance**. In all cases, security of the datasets reviewed to confirm the flow of the data in processing activities must be ensured.

Taking the above into consideration, once processing activities are clearly defined within the SLICES project, the **visualisation of the data processing flows** shall be performed. The data processing map that shall ultimately be drafted is meant to be periodically updated for optimal results and keeping current with any developments and changes in the organisational structure.

5.3. Personal Data Minimization Dilemma and Strategy

According to the principle of **data minimisation**, an organisation should limit the collection of personal data to what is directly relevant and necessary to accomplish a set of specific predetermined purposes. Accordingly, the data minimisation principle implies that data should not be retained any longer than required to attain the respective purposes.

Nonetheless, it is frequently noticed that there is a **discrepancy between data minimisation requirements and the necessity of retention**. Especially in the field of scientific research and experimentation, the dilemma is twofold; on one hand, **scientific research and the performance of experiments are notably lengthy procedures**, that may require an immense volume of data and yet may not be completed in the span of years. This engenders the need to store this substantial amount of information for a longer term than what the data minimisation principles may entail.

On the other hand, scientific research and the subsequent experiments present **preservation benefits** for societies as a whole, as they hold the potential to contribute to future research, serving as the basis for third parties' work fostering innovation and assisting in the further progress in the respective fields. Therefore, the results of such experiments may require publication and correlation to Digital Object Identifiers (DOI), in accordance with Open Science principles. Deliverables SLICES-DS D4.3 and D4.5 explain in detail Open Science and Fair requirements, as well as the project's participation to the European Open Science Cloud (EOSC).

In order to address the above-mentioned, it is generally recommended that **anonymised data** is used for such experiments, so as to avoid any potential violations of privacy and confidentiality rights of data subjects. **Adequate security measures and safeguards** to prevent de-anonymisation shall also be required.

Where anonymisation is not possible, a **selection of data** may be carried out, to distinguish vital information from redundant personal data. At all times, it is imperative that the **consent** of the data subject has been obtained, not only for the collection and processing of their personal data for the research's purposes, but also for the final publication of the results, providing them sufficient information beforehand to comprehend the nature of the data to be published, the audience that shall have access to it and the time period that their data shall remain available.

5.4. Personal Data Management

Personal Data Management may be defined as the application of policies and procedures involving personal data and metadata designed with a data governance framework. As such, the main elements to be determined within Personal Data Management are:

1. Which data and for which purposes are collected and processed,
2. How data shall be used, including how they shall be collected, produced and processed,
3. How and where data shall be stored, as well as the duration of retention,
4. Which metadata shall accompany the data,
5. Which data security and privacy protocols shall be implemented,
6. How to ensure data quality and accuracy,
7. Transferability of data.

Taking the above into consideration, the Data Management Plan (Deliverable SLICES-DS D4.1) has already recognised that personal data management within the SLICES project covers a **vast array of issues around personal data, including the establishment of a data governance framework, data quality assurances, metadata management, interoperability of data and alignment with not only data protection requirements but also the FAIR (Findable, Available, Interoperable, Reusable) data principles** and has already addressed them.

The Data Management Plan already established shall be **updated** once the data processing activities are duly finalised and shall be reviewed periodically in order to ensure **continuous compliance and effective policy implementation.**

6. Organisational Recommendations for SLICES

6.1. DPO

The SLICES projects shall adopt a **cooperative approach** as far as the DPO is concerned, as per Deliverable SLICES-DS D7.1. In particular, the network of DPOs shall work towards a **peer-reviewed data protection policy and procedure,** adopting a **layered approach to data protection**, with the aim of ensuring the highest level of compliance with data protection requirements. The project's DPO shall coordinate and oversee the operation of the testbeds' DPOs.

As part of their obligations, the **respective DPOs shall be responsible** for:

1) **Cooperating** with the rest of the DPOs on compliance matters,
2) Ensuring **compliance** with data protection requirements and performing monitoring activities,
3) **Training** staff involved with the personal data, where necessary,

4) Becoming a **point of contact** for experimenters, duly informing them about their obligations and possibilities using the testbeds,
5) Becoming an **additional point of contact for data subjects**, so that they can effectively exercise their legal rights,
6) Holding a **record of data processing activities**, **data subjects' requests, any potential breaches and counteractive measures,**
7) Contributing to **risk assessment reports and DPIAs**, while also overseeing their implementation,
8) Cooperating with the **supervisory national authorities**, where that is required.

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

The DPOs also maintain a high role in **managing data breaches**, notifying the data subjects involved, as well as competent authorities, where applicable. A **clear notification procedure** is established, along with a notification template, as per Deliverable SLICES-DS D7.1. The records maintained by the DPOs shall include such notifications, the level of risk, as well as the solution measures adopted.

The further DPOs' obligations shall be determined upon finalising the possibility of utilising personal data in the experiments or its exclusion thereof. In either case, the DPOs shall be responsible for ensuring that experimenters meet the personal data protection requirements or that they guarantee the abstention respectively.

6.2. Legal and Compliance Service

As already determined, SLICES intends to include a **Compliance Office** in its organisational structure that shall assist in compliance with legal and ethical requirements relevant for the SLICES project. As such, the Compliance Office shall be the **first point of reference for legal and compliance services**.

Among its **principal responsibilities**, as described in deliverable SLICES-DS D1.3, will be:

- The implementation and monitoring of an **effective legal compliance policy**,
- The **assessment** on a regular basis of the adherence to compliance requirements,
- The **audit** of the testbeds' activity to identify potential vulnerabilities, risks and threats,
- The **management of regulatory risks**,
- The **update** of the existing policy to match the latest regulations and compliance requirements,
- The **performance of staff training activities** to effectively communicate SLICES' ethical principles and legal policies,
- The **coordination** of actions as a **single point of contact** among the various testbed actors.

The Compliance Office shall **abide by the principles of autonomy, impartiality, transparency and accountability**, as the main principles relevant for the Office's activity.

A **record containing all legal policies and requirements**, as well as ethical standards for the SLICES project should be created and maintained by the Compliance Office. Said record is also advised to include a review of existing policies against current legislation and shall be periodically updated to keep up with the regulatory evolution.

6.3. DPIA and Risk Assessment

As described in the GDPR, a DPIA is a necessary tool to evaluate whether certain operations meet the data protection criteria prescribed by law. A DPIA is **particularly required in the following cases**: when sensitive data or data of a highly personal nature is involved, when data is processed on a large scale, when datasets from different operations are matched or combined and when new technological or organisational solutions are innovatively used or applied.

Similarly, a **risk assessment** is indispensable in order to **identify potential risks and threats** to the data subjects' rights and freedoms, **evaluate existing security measures and establish response and react framework.**

Both the above assessments shall be carried out **prior to processing**, in other words prior to the commencement of the SLICES testbeds operation. Nonetheless, both documents must be **regularly reviewed and updated** to maintain compliance with SLICES activities with data protection and security requirements. It is always advisable that the DPO is involved in the process of conducting the DPIA and risk assessment, as well as their maintenance and update.

The **DPIA** shall include, as a **minimum content,** the following information:

a. A thorough description of the data processing operations, as well as the purposes for which data is processed, the legal bases, lawfulness etc.,
b. The parties involved (controllers, processors etc.) involved in each data processing,
c. The obligations and tasks of each party involved,
d. A description of the data protection policy,
e. The level of protection of data subjects' rights,
f. A description of the data lifecycle,
g. The technical and organisational measures adopted,
h. The security measures adopted,
i. The certification mechanisms, seals and data protection marks that apply to the processing activities described,
j. The potential risks identified and their mitigation measures,
k. The date, signature and contact details of the project's DPO.

The **risk assessment**, in turn, shall review any potential risks to the freedoms and rights of individuals, which may include re-identification of pseudonymised data, cybersecurity threats and unauthorised access, loss of control over the use of personal data, the inability to exercise rights or the inability to access the services provided by the testbeds. As such, the risk assessment shall also detail the measures already adopted to combat any such risks, as well as recommendations to improve prevention strategy, as well as the react and respond framework.

It is noted that **publishing the DPIA and the risk assessment** is not legally required by the GDPR. However, it could be useful for the SLICES project to publish part of the assessments or a summary, as a means to demonstrate a high level of accountability, transparency and responsibility, enhancing trust in the SLICES' operations.

7. Proposed SLICES Data Protection Policies

7.1. Regular Monitoring and Compliance Assessment

In order to achieve long-term compliance, it is vital that data protection policies, established procedures and mechanisms, as well as the technical and organisational 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.

In particular, monitoring shall be perceived as the **continuous control on the policy and actual implementation within the project** to ensure that personal data remains protected from potential external or internal risks and threats. To that end, **any changes in regulations and applicable legislation shall also be monitored**. If new legislation is put into force, SLICES policies shall be adapted to the latest changes to ensure continuous compliance. Additionally, the SLICES staff shall also be subject to training on updated legislation.

At the same time, an adequate **procedure of notification** shall be established, where third parties and members of the SLICES project shall be able **to inform the DPO of any identified compliance risks and threats via email.** The DPO shall maintain a **record of such notification**, along with their own evaluation of the situation, their findings, mitigation measures and the final solution.

Last but not least, a **compliance assessment** shall be performed **regularly**, and at least on an annual basis. Said assessment shall **include all existing policies, rules, procedures, security mechanisms and technical and organisational measures**, which shall be reviewed **against current legislation and requirements in terms of their effectiveness** in protecting personal data. Interviews with staff members may also be conducted if deemed necessary, while access to the DPOs' records shall be provided.

Below there is an **indicative list of steps** to be followed for an efficient compliance assessment:

1) Review of the **current legislation and guidelines**,
2) Review of **existing policies, rules and procedures**,
3) Identification and mapping of **potential compliance risks and gaps,**
4) Identification of **existing security measures**,
5) Assessment of **controls in place** to prevent, detect and correct compliance risks,
6) Recommendation of **further mitigation measures or adaptations**,
7) Regular **updates** of the risk assessment.

7.2. Consent Management

Given the always-increasing role of consent within current data protection frameworks, it is understandable that consent management remains **one of the most crucial points** for any organisation involving personal data for any of its operations. As such, consent management is precisely the process that shall guide compliance with legal consent requirements, required to collect, process and store data subjects' personal information.

Consent is one of the principal six lawful bases provided by the GDPR to collect and process personal data and must meet a number of conditions laid out in Article 7 of the GDPR. In particular, consent must be:

a. **Informed**, having provided the necessary information to the data subjects prior to their consent, in particular referring to which data shall be collected and processed, for which purposes, how it will be used, who shall have access to it, any possible risks for the data subjects, as well as the necessary information regarding their rights, including the right to withdraw consent,
b. **Specific**, for the exact purposes already known to the data subject,
c. **Given freely**, implying a real choice for data subjects with no elements of external pressure, influence or power imbalance, while withdrawal must be possible without detriment for the data subject,
d. A **clear and unambiguous indication of the data subjects' wishes,** thus requiring an affirmative act of consent and not a pre-ticked opt-in option.

Taking the above into consideration, it is essential that the SLICES testbeds provide the necessary **information of consent prior to the testbeds' utilisation**. Such information shall involve, at a first layer, the information that shall be collected and processed on experimenters registering in the platform, as well as subscribers to receive communication regarding the SLICES project. At the same time, consent to cookies is also included in this level.

For this layer of consent, SLICES shall ensure that information regarding the data that shall be collected in each case is duly provided to data subjects prior to the actual collection and processing of their data. Said information shall be provided in a **clear and transparent manner**, explaining sufficiently the precise results of providing consent, including the data retention period and the actions once said period expires, such as deletion of data. Once that has been accomplished, the data subject must be given the **choice to clearly consent** to the collection and processing of their data by a clear affirmative action. A predetermined opt-in function that can be ticked off at a later stage is not sufficient. Where consent is required for more than one purposes, it should be provided separately for each purpose in a granular form.

At a second level, **consent may also involve personal data input by the experimenters**, in case the testbeds decide to allow such action. In this case, it is the experimenters that shall ensure that they meet the conditions of consent for any data they intend to utilise in their experiments via the testbeds. For this reason, they shall be liable to provide guarantees to SLICES that they have legally obtained consent for the purpose of conducting their experiments via the testbeds.

Once adequate consents have been collected, they shall be **stored at a secure repository** for future reference, to facilitate the exercise of data subjects' rights, as well as to be able to demonstrate compliance with the necessary data protection requirements.

7.3. Security

The security is an essential point to take into account during the design, deployment and operation of the SLICES Research Infrastructure. To ensure the correct enforcement of the security and also the trust, security and trust management policies have been elaborated and are presented in this section.

These policies should be applied by the testbed providers and the experimenters when using the different tools and services available through the SLICES Research Infrastructure. The objectives of the security and trust management policies are to guarantee any circumstances the confidentiality, integrity and availability (the famous CIA triad) during the operation on the SLICES Research Infrastructure.

First of all, the access to the components of the SLICES Research Infrastructure and to the data generated or managed by these components is limited to authenticated and authorised people. Concretely, it means that only the members of SLICES can access the most critical parts of the SLICES core, depending on their function and roles inside the SLICES entity. For instance, the engineers in charge of the maintenance of the SLICES Research Infrastructure have sufficient access rights to proceed to the necessary updates, notably those dedicated to the security. On the other hand, administrative workers will not be granted to access the technical parts of the SLICES Research Infrastructure. In summary, the principle of least privilege (PoLP) will be applied to each element of the SLICES Research Infrastructure to reduce the security risks. An element can be for example a program, a service, a resource or a dataset. Typically, a user will be able to access only the necessary information and/or services based on a legitimate purpose. The data should be classified and labelled in function of their confidentiality or sensitivity. The physical and virtual accesses should be limited to the authenticated and authorised people in function of their roles in SLICES. Each person working for or using the SLICES Research Infrastructure is responsible to apply the security and trust management policies based on the access rights and roles he received from the SLICES Research Infrastructure management. Training activities are to be put in place to inform the people involved in SLICES how to correctly deal with the security and the data protection, notably by explaining the security best practices in the ICT domain.

An important point in the context of SLICES is to ensure the integrity of the data. The data should be trustworthy and free for tampering. SLICES should maintain the data only if the datasets are authentic, reliable and accurate. The integrity of the data can be ensured by different technical mechanisms like hashing, encryption and digital signatures. Furthermore, each node of the SLICES Research Infrastructure should be trustable by the experimenters. In this context, the creation and the utilisation of recognised certificates by every node are a good mechanism to enforce the trustworthiness. Exchanges of data will be possible only if there are valid certificates and the data are encrypted to avoid any interception during the transit of data. Furthermore, secure protocols such as IPSec, SSL and TLS (used typically for HTTPS) are mandatory for the data transmissions. Network security standards used for the transmission of data should be announced and applied by the different nodes of SLICES.

The availability should guarantee that getting datasets or other kinds of information in the SLICES Research Infrastructure doesn't take a large amount of time. It means that some 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. Backups and contingency plans should be organised properly in case of incidents of different natures. Data backup requirements should be established in the different nodes involved in the SLICES Research Infrastructure.

Of course, the security and trust management policies are based on the current regulations on data protection mentioned in this document. These policies will be reviewed and adapted following the process described in section 8.7 of this document.

7.4. Cross-border and international Data Transfers

In the era of increased interconnectivity, data transfers are one of the elements most affected by the GDPR. In particular for SLICES, aiming at creating a globally accessed environment of interconnected devices, taking full advantage of emerging technologies, data transfers are an essential component of its daily operations and must ensure the protection of personal data.

One of the main GDPR distinctions regarding data transfers is between **adequate, where no prior approval by the supervisory authority is required, and non-adequate countries, where additional safeguards must be placed**. Examples of such countries regarded as **adequate include the UK and Switzerland**. Of course, cross-border data transfers when involving the EU Member States, as well as Norway, Liechtenstein and Iceland, do not fall within the scope of international data transfers for which additional measures must be taken, but it is still required that security and the data subjects' rights are respected.

Taking the above into consideration, the first step toward safe data transfers lies in verifying whether an **adequacy decision by the European Commission** exists, taking into account the country's upholding of the rule of law, human rights and fundamental freedoms, its personal data protection legislation, the independence of its national supervisory authorities, as well as the international commitments of the country on data protection.

If no such decision has been made, data transfers are subject to a number of **additional safeguards** intended to protect data subjects' privacy and personal data, enabling them to effectively exercise their rights, including access to effective legal remedies. Such safeguards shall be **included in the required data transfers agreement** to be signed between the SLICES project and the entity located outside of EU territory and may include binding corporate rules, codes of conduct or recognised certification.

Additionally, **one of the following conditions must be met**:

i) The data subject has explicitly consented, or
ii) The transfer is required for the performance of a contract between the data subject and the controller, or
iii) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject, or
iv) The transfer serves important public interest reasons,
v) The transfer is necessary for the establishment, exercise or defence of legal claims, or
vi) The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

Data subjects shall be informed in advance regarding the categories of personal data that shall be transferred, the standard contractual clauses, access rights, any security measures in place, as well as how they can exercise their rights.

In addition to the above, the **data transfer agreements shall clearly describe:**

- The data shared,
- The purposes of the data transfer,
- A clear allocation of responsibilities and rights among the parties,
- The exact transfer methods, ensuring security of the data throughout the entire transfer,
- Where data shall be stored and who shall have access to it,
- The precise security measures in place,
- The data subjects' rights and how they can exercise them,
- The protocols regarding security incidents and breach managements,
- Liability clauses,
- The receiving parties' data protection standards,

- Notification requirements.

Any data transfers performed within the SLICES project shall ensure that the standards set out by the GDPR, as well as further EU legislation on the protection of data shall be upheld.

7.5. Web Interface and Cookies Policy

Upon final definition of the service range to be provided by the SLICES project and its associated user interfaces, the project must generate tailored solutions manage user preferences and enable user right management. Furthermore, it is recommended that the project follows best practices for end-user accessibility throughout its design and development phase. A tailored Cookies and Privacy policy for the platform should also be provided.

7.6. License policies and other considerations

A common understanding of licensing policies is integral to facilitating in-depth understanding and integration into research infrastructures. This section provides a suggested license policy framework enabling the further analysis of policy needs and objectives.

7.6.1. General requirements

Before further detailing license policy-specific requirements, this subsection will briefly explain what policies are in general and what requirements are tied to them that ensure their successful operation within the given organisational context. This baseline supports the generation of license policies and serves as a building block.

Policies can be defined in numerous ways but in the context of this deliverable, we refer to policies as formal documents containing organisational rules, operating methods, or best practices to be followed and targeted toward the personnel of an organisation. Although most policies are written, there can be unwritten or de-facto procedures and practices present.

As shown in the following figure and explained further below, numerous characteristics are relevant for the construction of organisational policies:

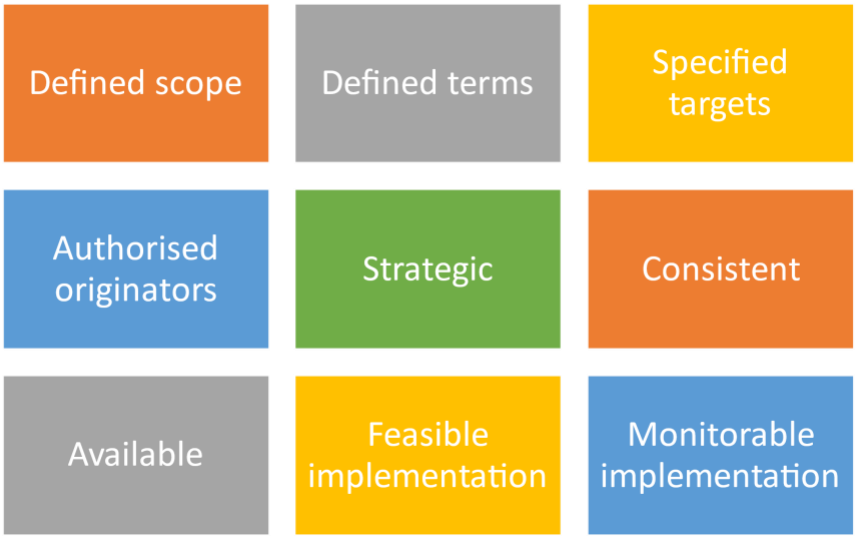


Figure 1: General policy requirements

In simple terms, 9 crucial building blocks must be considered when designing a policy:

1. Policies must have a clearly **defined scope**, including mandates, actions and relationships to control, positions to be affected, as well as time limits or renewal periods.
2. The **terms** utilised in the policy must be clearly **defined** and properly referenced to facilitate understanding of the readers, without the unnecessary use of jargon or technical terms.
3. Policies must **specify** the **target** group of people to whom the policy is addressed. The target group of people can be understood as a specific position here rather than a specific person to avoid the changing of policies with any personnel change.
4. **Originators** of policies must be **authorised** to make their policies, including clearly documented authorship.
5. Policies must be aligned with the given organisational **strategy** and not conflict with organisational missions, plans or visions.
6. Policies must be **consistent** with external policies related to research infrastructures and relevant regulations.
7. Policies must be made openly **available** and accessible, including on either internal or external webpages with the applicable metadata.
8. The **implementation** of these policies must be **feasible**; policies must be developed keeping in mind the available resources, as well as the organisational strategy, and external regulations.
9. Policies must be **monitorable** to ensure sound implementation and consistent application.

7.6.2. License policy-specific requirements

Apart from the generic requirements of policy framework, license policies have an additional layer of constraints to take into account. Licenses are necessary to ensure that the (meta)data provided is used in a pre-defined manner, keeping users not only informed on how their data is used but also enabling the interoperability of services.

In general, open licenses are the most common form of license policies within organisations. They must adhere to not only technology specific licenses but often need to follow specific national or local guidelines, making harmonisation and the introduction of single licenses problematic. Nonetheless, for

license policies to be effective, particularly in ensuring interoperability, they must observe certain requirements. This list includes:

Datasets definition: Currently, there are many definitions available to define datasets based on various factors, such as the type of the RI, subdomain requirements, dataset selection, etc. Harmonised definition of datasets or at least a framework solution with a list of definitions supports interoperability.

Defined data version: Versioning of datasets is crucial for ensuring continuous improvement and reusability. There must be a clear methodology or strategy implemented to communicate data changes.

Machine-readable: Machine readability enables the interoperability and findability of data. Therefore, it is important to select license policies that apply to the datasets used, enabling interoperability and compatibility.

Metadata license: Metadata is often considered part of data and, therefore, the same license policy applies to it. However, if the origin of the metadata differs from the data, a different license applies. This is an important consideration for RIs; they must ensure that the metadata has its own license policy where applicable and that this license includes quality control measures. Here, metadata standards are also crucial for the reusability of such data.

Unique identifier: Following the FAIR principles, each dataset must have a unique identifier (persistent identifier). Therefore, a clear policy is required on their definition.

Data access: An access policy detailing in a transparent manner the data access mechanism and access protocols must be a vital part of policies. Where relevant, this section should detail access to restricted data with supportive ethical guidelines, review process, and corrective actions.

Retention: Data repositories retain data and metadata; in this context, it is important to apply specific provisions for the sustainability, usefulness and trustworthiness of data. It is important to have specific measures in place ensuring that the volume of data and metadata is reduced where and when applicable, based on a set timeframe included in the license policy.

Ownership: Ownership and licensing agreements with data providers ensure that the necessary permissions can be granted.

Service level agreements: Service level agreements ensure the quality of the provided service in the context of data use.

7.6.3. License policy-specific requirements

One of the key challenges related to (license) policies relates to the lack of harmonisation between available frameworks, as well as the necessity to often apply national or local licenses. Additionally, the license standardisation landscape is also vast, making it difficult to find the best solutions on the market and avoiding having too many policies in place with overlaps.

7.7. Periodic Policies Review

A **periodic policies review** is a recommended method, offering the opportunity to reflect on existing policies, their effectiveness, as well as any room for further improvement. This is particularly vital for high-risk and high-regulated sectors, such as those involving Artificial Intelligence, healthcare etc. Such review is **essential to verify the following**:

a. Whether the policy is effective,
b. Whether the policy is duly implemented,
c. Whether the policy remains necessary, clear and accurate,
d. Whether the policy is up to date with current legislation,
e. Whether the policy still reflects the goals and objectives of the project.

The policy review can be made **independently or in conjunction with the compliance assessment**, as the results of the latter can form the foundation of the review, the amendments necessary and any additional requirements. As an independent review, it can be based on an analysis of existing policy, the study of new legislative initiatives, guidelines and best practices, stakeholders' recommendations as well as the users' and data subjects' comments, complaints or notifications. In all cases, the policies review shall bear in mind their impact to users, data subjects, Consortium members and the SLICES project as a unit.

Such policies review **shall include all policies developed under the SLICES project**, namely the licensing policy, data protection policy, cookie policy and the terms and conditions of the testbeds. Since policy review is most effective when performed regularly, the review period shall be reasonable to proactively verify compliance, and at least on an annual basis. Of course, in case of impending or already performed amendments in legislation, organisational changes or other incident, the policies **may be reviewed outside the predetermined review framework in response to the event that rendered them necessary.**

8. Conclusion

8.1. Main Takeaways

Having reviewed applicable legal requirements for the SLICES project in terms of personal data, it is evident that implementing **effective data protection policies is of utmost importance** for the evolution of the project. In fact, data protection **shall be considered not only by the SLICES consortium, but also by experimenters utilising the platforms** developed.

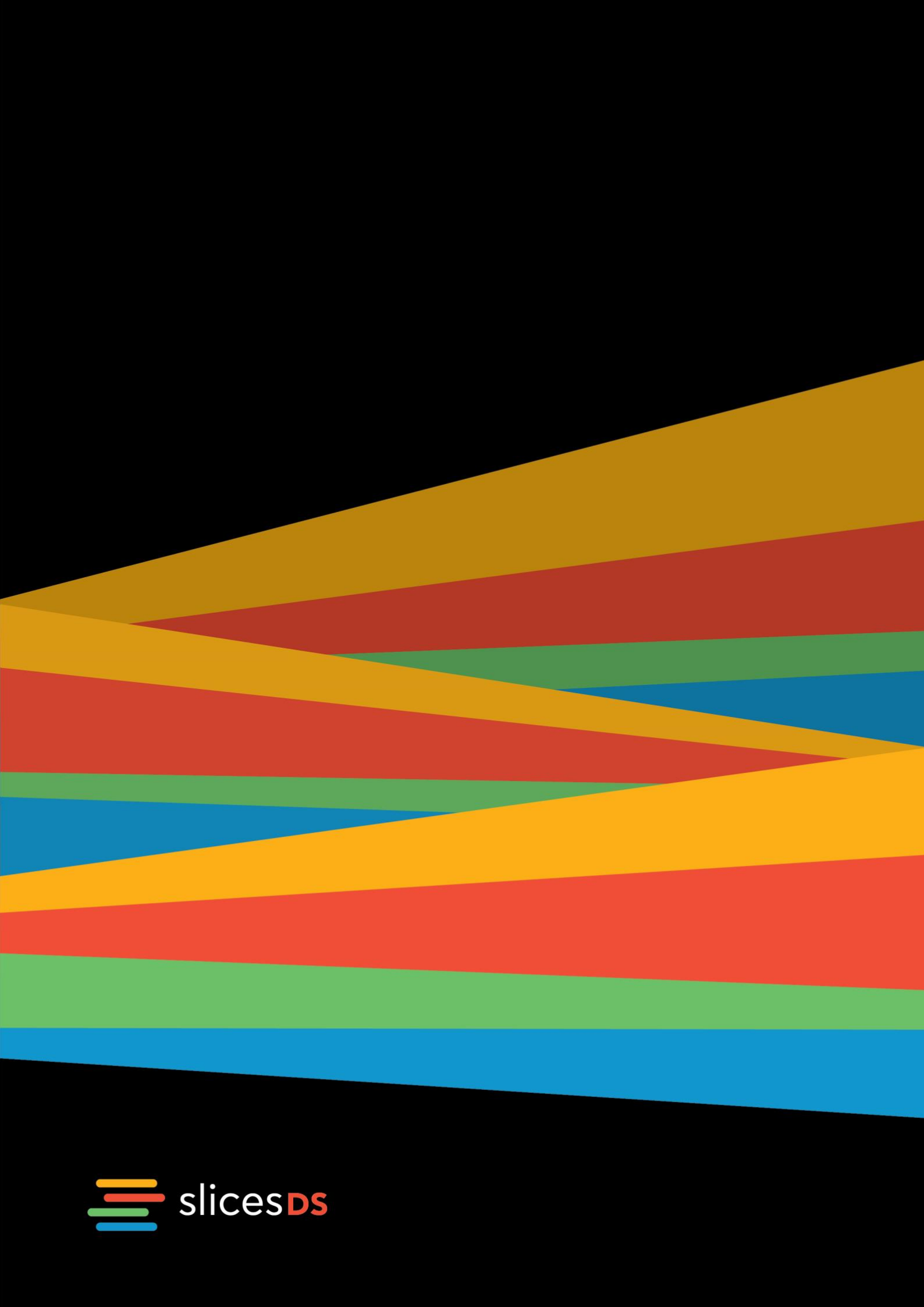
SLICES shall be **supported by the project's DPO and the network of DPOs** that will be established, as well as the **Compliance Office**, with the aim of ensuring compliance with the necessary legal requirements, reviewing existing policies, managing data requests and performing Data Protection Impact Assessments and Risk Analyses for the proper and smooth operation of the project.

The **policies** that will be developed shortly prior the project's operation will cover a **large array of subjects**, ranging from data protection per se and the management of data subjects' consent, the design of the web interface and the application of cookies to security measures and the licensing of the data involved. Naturally, the policies will be **regularly reviewed to maintain the high level of compliance that will be established from the initial stages, in accordance with data protection by default and by design principles.**

As the project progresses, the above mechanisms, policies and bodies will be finalised to better reflect SLICES' vision, as well as its intended operations, services and possibilities.

8.2. Actions for SLICES-SC and SLICES-PP

The present deliverable, as well as its assessments, findings and guidelines remain relevant within the context of SLICES-RI, including its existing and future sub-projects. As per the privacy by design and by default approach that SLICES has adopted, the content and outcomes of this deliverable need to be considered for all future SLICES steps and throughout its lifecycle to ensure compliance with personal data protection requirements. Data protection policies shall be adjusted to fit the project's needs in each step, as well as to incorporate any amendments or additions to the existing legislation.


slicesDS