Research and Innovation Action

Social Sciences & Humanities Open Cloud

Project Number: 823782 Start Date of Project: 01/01/2019 Duration: 40 months

Deliverable 5.8 Draft SSH GDPR Code of Conduct

Dissemination Level	PU
Due Date of Deliverable	30/06/2021 (M30)
Actual Submission Date	10/08/2021
Work Package	WP 5 Innovation in Data Access
Task	Task 5.3 Legal Issues of Innovative Data Access
Type	Report
Approval Status	Waiting EC approval
Version	V1.3
Number of Pages	p.1 – p.57

Abstract:

SSHOC Deliverable 5.8 intents to create a draft of SSH GDPR Code of Conduct. It describes what a Code of Conduct entails, the purpose of creating one, and terms for creating it. It also provides suggestions to what a SSH GDPR Code of Conduct draft might contain, who such a code can be relevant for (within the SSH community) and addresses which actions are considered necessary to initiate further development of SSH GDPR Code of Conduct in SSHOC WP8.

The information in this document reflects only the author's views and the European Community is not liable for any use that may be made of the information contained therein. The information in this document is provided "as is" without guarantee or warranty of any kind, express or implied, including but not limited to the fitness of the information for a particular purpose. The user thereof uses the information at his/ her sole risk and liability.

SSHOC, "Social Sciences and Humanities Open Cloud", has received funding from the EU Horizon 2020 Research and Innovation Programme (2014-2020); H2020-INFRAEOSC-04-2018, under the agreement No. 823782

History

Version	Date	Reason	Revised by
1.0	14/06/2021	First draft	Authors
1.1	30/06/2021	Revised Draft	Vanja Komljenovic/Ivana Ilijasic Versic
1.3	09/08/2021	Final version for submission	Ivana Ilijasic Versic

Author List

Organisation	Name	Contact Information
NSD	Ina Nepstad	Ina.nepstad@nsd.no
NSD	Inga Brautaset	Inga.brautaset@nsd.no
NSD	Mathilde Steinsvåg Hansen	Mathilde.hansen@nsd.no
NSD	Tore A. K. Fjeldsbø	Tore.Fjeldsbo@nsd.no
NSD	Siri Tenden	Siri.Tenden@nsd.no
NSD	Marita Ådnanes Helleland	Marita.Helleland@nsd.no
NSD	Christopher Ongre Autzen	Christopher.Autzen@nsd.no
NSD	Ingvild Eide Graff	Ingvild.Graff@nsd.no
NSD	Marianne Høgetveit Myhren	Marianne.Myhren@nsd.no
NSD	Vigdis Namtvedt Kvalheim	Vigdis.Kvalheim@nsd.no

Executive Summary

The General Data Protection Regulation (EU) 2016/679 (hereinafter GDPR or this Regulation) has given European countries a unique opportunity to harmonise their legal framework, and to improve the conditions for research and cross-border data flow. Although one of the rationales behind the GDPR was to harmonise the legal framework for data processing to improve conditions for research and cross-border data flow, this has not necessarily been the case.

To facilitate harmonisation across EU/EEA and sectors, the EU Commission has highlighted creation and use of Codes of Conducts as an important tool to ensure such harmonisation[1]. A Social Science and Humanities (hereinafter SSH) GDPR Code of Conduct may lead to such a harmonised practice within the SSH environment. The main aim of this deliverable is to initiate the work on enabling the creation of a draft SSH GDPR Code of Conduct.

This Deliverable, 5.8, is a part of Task 5.3, Work Package (hereinafter WP) 5 within SSHOC. In Task 5.3, Legal Issues of Innovative Data Access, Deliverable 5.7, the impact of the GDPR and its possible implications for cross-border research have been analysed. The task team also arranged a SSH GDPR Code of Conduct Stakeholder workshop in March 2021. This workshop has been reported, as part of Deliverable 5.19. The task team`s understanding of Deliverable 5.8, is to start the initiative of creating a SSH GDPR Code of Conduct draft, by explaining what a Code of Conduct is, what it entails, and the purpose and benefits of creating a SSH GDPR Code of Conduct. This will be performed by e.g., literature studies, to get a better understanding of the scope of focus. This is intended to strengthen the will of creation of a SSH GDPR Code of Conduct draft in the SSH Environment. Further, the deliverable explains which terms must be fulfilled to be able to create and get a SSH GDPR Code of Conduct draft admissible. The Deliverable also provides some suggestions for what a SSH GDPR Code of Conduct draft may regulate.

As the deliverable highlights, significant actions remain needed before a SSH GDPR Code of Conduct draft can be finalised, including planning how to fulfil all terms in order to get a SSH GDPR Code of Conduct admissible and organized. However, it also specifies the benefits of doing the work and why the SSH environment should be motivated to get involved in the upcoming work.

To conclude, SSH GDPR Codes of Conduct contributes to research taking place within the framework of regulations. The GDPR is general and applies to all processing of personal data. A SSH GDPR Code of Conduct can explain how processing of personal data within the SSH environment can be carried out in

[1] Report from the European Commission (2020), "Two years of the GDPR: Questions and answers", accessible at: https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1166, (12.08.2020)

accordance with this Regulation. Without Codes of Conduct within the field of research, European cooperation can be demanding. It can be virtually impossible to collect large amounts of research data for long-term storage and sharing across European countries. Such a consequence will not only be a loss for research, but also for the society. The deliverable is a part of Task 5.3 Legal Issues of Innovative Data Access, Work package (hereinafter WP) 5 Innovation in Data Access, and will be further developed in Task 8.3, WP 8 of SSHOC. In this deliverable the task team addresses what a Code of Conduct is, what it entails, why it can be helpful, what a SSH GDPR Code might regulate, and which assessments and actions needs to be taken to enable a SSH GDPR Code of Conduct draft to be created. By doing this, the task team intend to facilitate and suggest how the initiative can be further developed in WP8 - Governance/ Sustainability/ Quality Assurance, T.8.3 Legal and Ethical issues. The task team also address some suggestions on what a SSH Code of Conduct might regulate. However, the scope and purpose of the SSH GDPR Code of Conduct can`t be decided by the task team, at the procedures for developing a Code of Conduct indicated that this must be jointly decided within the SSH Environment[2]. The task team therefore suggests that different Stakeholders within the SSH Environment should be consulted in the upcoming work in Task 8.3. Different suggestions and opinions on what a SSH GDOR Code of Conduct should regulate must thereafter be assessed, when determining the scope of the Code.

[2] EDPB’s Guidelines, chapter 5, accessible at: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_en.pdf

Abbreviations and Acronyms

BBMRI ERIC	European research infrastructure consortium (ERIC) for biobanking; https://www.bbmri-eric.eu/about/
CoC	Code of Conduct
Data controller	The data controller determines the purpose for which and means by which the personal data are processed (why and how the data are processed). The data controller is responsible for complying with data protection legislation.
Data processor	A data processor is a person or company outside the data controller's organization, which processes personal data on behalf of the data controller. The law requires that this relationship be regulated by agreement.
EC	The European Commission
EDPB	European Data Protection Board
EEA	European Economic Area
EOSC	European Open Science Cloud
EU	European Union
GDPR	The General Data Protection Regulation (EU) 2016/679
NSD	Norwegian centre for research data
SSH	Social Science and Humanities
SSHOC	Social Science and Humanities Open Cloud
WP	Work package

Table of Contents

1. Introduction

The main purpose of SSHOC is to create the social sciences and humanities area of the European Open Science Cloud (EOSC) thereby facilitating access to flexible, scalable research data and related services streamlined to the precise needs of the Social Science and Humanities (hereinafter SSH) community[3]. The research data of interest often contain personal data.

Personal data means all data related to an identified or identifiable person ("data subject"). This can include directly identifiable data, such as names or mail addresses, or indirectly identifiable data, by combining variables or usage of a scrambling key. This can also include processing of pseudonymised data, meaning data not containing indirectly or directly identifiable variables, but linked to a scrambling key, where reidentification is possible 4 . All processing activities related to such data must be in accordance with data protection regulation.

The term "processing" means all operations or set of operations performed on personal data or on sets of personal data, such as gathering, storage, recording, making available, analysing, transferring of personal data5. All such processing activities of research data containing personal data, will therefore be subject to data protection regulation. The General Data Protection Regulation (EU) 2016/679 6 (hereinafter GDPR or this Regulation) regulates the processing of personal data within EU/EEA.

As the GDPR applies to processing of personal data throughout EU/EEA, the GDPR has given most European countries a unique opportunity to harmonise their legal framework, and to improve the conditions for research and cross-border data flow. One of the rationales behind GDPR is to ensure the same level of data protection throughout Europe to facilitate open access and reusability of research data.

According to the report «Two years of the GDPR: Questions and answers"[7], published on 24 of June 2020 by the EU Commission, the implementation of the GDPR has been a success. The report concludes that harmonisation across the Member States is increasing, although there is a certain level of fragmentation that must be continually monitored. Furthermore, the report states that it is important to further support harmonisation and consistent implementation of the GDPR across the EU. This includes making sure that national legislation is fully in line with the GDPR. To facilitate harmonisation across Member States and

[3] SSHOC project, accessible at: https://sshopencloud.eu/ (accessed Aug 2021)

[4] GDPR, Art. 4 (5), accessible at: https://gdpr-info.eu/

[5] Op.cit., GDPR, Art. 4 (2)

[6] The General Data Protection Act, accessible at: https://gdpr-info.eu/

[7] Op.cit., Report from the European Commission (2020), "Two years of the GDPR: Questions and answers"

sectors, the report highlights creation and use of Codes of Conducts as an important tool to ensure such harmonisation.

The task members have been assigned with work to support the main purpose of SSHOC to be archived, and the WP 5`s overall aim is to facilitate innovations in data access and to provide tools and services for intelligently open data for the SSH domain to be incorporated into the European Open Social Science Cloud (hereinafter EOSC). Task 5. 3 address legal and ethical issues related to open access, reusability of research data, and legal implication of the FAIR principles.

In Task 5.3, Deliverable 5.7, the impact of the GDPR and its possible implications for cross border research, has been analysed. The task team also arranged a SSH GDPR Code of Conduct Stakeholder workshop[8]. This workshop has been reported, as part of Deliverable 5.19. The overall aim is to initiate the work on a SSH GDPR Code of Conduct to be handed over to and finalised in T8.3, within WP8.

Findings in SSHOC Deliverables, 5.7 and Deliverable 5.19 may indicate that the GDPR has not been successfully implemented in the field of research, and consequently not ensured the desired harmonised practice within Europe. The terms and conditions for processing personal data for research purposed seems to differ from one country to another, thus making it more challenging to share personal data across borders. The interpretation of the Regulation seems to differ in the research community throughout the European countries. In addition, in cases where the Regulation leaves room for interpretations, it is indicated that ethical consideration can affect which solutions to be taken. One example can be the use of consent as lawful ground for processing of personal data, instead of a public interest/ scientific purposes. It is important to address findings in Deliverable 5.7 and 5.19 cannot be generalised to represent all European countries, as it only interpretate legislation within a few selected countries, and present the understanding of random selection of people (n<50) within the research environment in these countries.

To facilitate harmonisation across the European SSH research environment, this Deliverable intend to start the initiative, leading to the creation of a SSH GDPR Code of Conduct draft. The GDPR encourages the use of approved Codes of Conducts as a tool to ensure correct legal application and demonstrate compliance with the GDPR[9]. This gives the SSH environment an opportunity to create a formal common framework to demonstrate compliance and facilitate harmonisation of data-sharing rules and practices.

[8] SSHOC GDPR workshop, accessible at: https://zenodo.org/record/4655623#.YNrBnukzZp8 (accessed Aug 2021)

[9] Op.cit., GDPR Art. 40

1.1 Methodology

Deliverable 5.8 is a part of Task 5.3, which address legal and ethical issues related to open access, reusability of research data, and legal implication of the FAIR principles.

The description of Deliverable 5. 8 is to "draft SSH GDPR Code of Conduct (Legal issues of innovative data access) (...) and provide input to WP8.3 Ethical and Legal Issues thus making a first draft of a common SSH GDPR Code of Conduct".

The task team`s understanding of the task is to start the initiative of creating a SSH GDPR Code of Conduct draft, by explaining what a Code of Conduct is, what it entails, and the purpose and benefits of creating a SSH GDPR Code of Conduct. This is intended to strengthen the will of creation of a SSH GDPR Code of Conduct draft in the SSH Environment.

Further, the deliverable explains which terms must be fulfilled to be able to create and get a SSH GDPR Code of Conduct draft admissible. This has been considered necessary by the task team, as multiple procedural actions must be taken to enable a SSH GDPR Code of Conduct draft to be evaluated and considered admissible. The terms/procedural steps presented in 3.2 are set to enable an effective evaluation on any Code of Conduct draft10 , and will therefore be relevant for the further initiative to be taken within WP8. Section 3.2 in this Deliverable presents the terms to get a Code of Conduct draft admissible. This is based on interpretation of the relevant articles in GDPR, and guidelines presented by the European Data Protection Board (hereinafter EDPB).

The Deliverable also provides some suggestions for what a SSH GDPR Code of Conduct draft may regulate, leaning among others on results from Deliverable 5.7 and 5.19 and the BBMRI-ERIC`s work on a health and life Science GDPR Code of Conduct. However, it is important to highlight that some of the terms/procedural steps can affect what the SSH GDPR Code of Conduct draft can contain. A plan must be made on how to fulfil these terms, and this deliverable does not present a first version of a SSH GDPR Code of Conduct draft. It is the task team`s understanding that it cannot decide what a SSH GDPR Code of Conduct draft can regulate, as the procedures for developing a Code of Conduct indicates that this must be jointly decided within the SSH Environment[11]. Different stakeholders must be consulted[12], and other suggestions and opinions on what a SSH GDPR Code of Conduct should regulate, can be relevant to include once the initiate progress within the SSH Environment and Task 8.3. When and how the SSH

[10] Op.cit., EDPB's Guidelines, section 19

[11] Op.cit., GDPR, chapter 5

[12] Op.cit., GDPR, section 28

GDPR Code of Conduct draft should be written, must be further elaborated in WP8, Task 8.3. The same applies for deciding the content of the code draft.

The initiative laid down in this Deliverable, represents therefore a starting point of the initiative, and will need a significant collaboration between stakeholders within the SSH environment to enable the draft to be written and submitted. As this Deliverable highlights, significant actions remain before a SSH GDPR Code of Conduct draft can be finalised. However, it also specifies the benefits of doing the work and why the SSH environment should be motivated to get involved in the upcoming work with preparing a draft SSH GDPR Code of Conduct.

2. What is a Code of Conduct and what is the purpose of having one?

2.1 Introduction

A Code of Conduct, under the GDPR, is a set of rules that assist members of that Code with data protection compliance and accountability in specific sectors or relating to processing operations[13]. Code of Conducts can help organisations to ensure they follow best practice and rules designed specifically for their sector or processing operations, thereby amplifying compliance with data protection laws. Code of Conduct are developed and managed by an association or institution, with the expert and sectoral knowledge of how to enhance data protection in their area[14]. A Code of Conduct helps to narrow down what the law means for a specific sector (e.g., research), i.e., they enable a sector to own and resolve key data protection challenges. It can provide a practical guidance in clear and simple terms with examples taken from the industry on how the GDPR applies[15].

The rules on Codes of Conduct are described in the GDPR art. 40 and 41, stating that: “The Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of Codes of Conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.” [16]

[13] Op.cit., GDPR, Art. 40

[14] Op.cit., EDPB`s Guidelines, chapter 3

[15] Ibidem

[16] Op.cit., GDPR, Art. 40

The GDPR thus emphasizes that Codes of Conduct should be a practical help for companies in how to comply with the privacy rules[17]. Codes are important components in broadening and adapting the tools for data protection compliance that controllers and processors can draw on, by way of a "semi-self-regulating" mechanism. A Code of Conduct intends to:

- Contribute to the proper application of the Regulation[18]
- Be adapted to the special conditions in each industry / sector[19]
- Consider the special needs of small and medium-sized enterprises[20].

In summary, a Code of Conduct is a set of rules for a specific industry, which provides specific guidelines for how companies must adapt to comply with the requirements of the GDPR[21]. A Code of Conduct is developed by the industry itself and approved by the national Data Protection Authority[22]. However, a GDPR Code of Conduct is more than just a guidance or best practice document, and it must specify or enhance the application of data protection law to a defined sector or processing activity[23]. Hence, a Code of Conduct should not merely be a restatement of the GDPR. Codes are expected to provide benefit for their sector, as they will address the requirements specific to the sector or area of data processing. They could be a cost-effective means to enable compliance for a sector and its members[24].

When the GDPR provides rules on Codes of Conduct, one of the main purposes is to make it easier for companies in various areas of society to comply with privacy legislation[25]. The GDPR is designed for all processing of personal data. At the same time, each industry encounters specific issues regarding how privacy legislation is to be implemented in practice. The GDPR therefore allows for - and in fact encourages - various industries to draw up standards of Conduct[26]. The Code of Conduct should be practical aids that help companies to apply the privacy rules in everyday life.

A Code of Conduct must be well established in the industry that is to use it. The initiative and the preparation of Codes of Conduct must therefore be done by institutions that represent the industry[27]. A

[17] Ibidem
[18] Ibidem
[19] Ibidem
[20]Op.cit., EDPB`s Guidelines, chapter 4
[21] Op.cit., EDBP`s Guidelines, chapter 3
[22] Op.cit., GDPR, Art. 40(5)
[23] Op.cit., EDPB`s guidelines section 23
[24] Op.cit., EDPB`s Guidelines chapter 3
[25] Op.cit., EDPB`s Guidelines, chapter 1
[26] Op.cit., GDPR, Art. 40(1)
[27] Op.cit., Art. 40 (2)

broad involvement (reference group) from the industry is also imposed in the process of developing a Code of Conduct[28]. The idea is that the industry itself is best suited to know what challenges needs to be addressed regarding the interpretation of the privacy regulations, and in which areas it is difficult to understand what the regulations says. According to the GDPR, a business/ organisation is responsible for complying with all data protection principles and is also responsible for demonstrating compliance[29]. The industry itself should therefore develop its own sector-specific aids to safeguard privacy in line with the law.

The Codes of Conduct shall contribute to the operationalisation of the regulations[30]. It is therefore central that the Code of Conduct is designed as a practical tool that, in a concrete manner, explain how the regulation is applied in a specific area. The Codes of Conduct should function as a guideline in everyday life. The Code of Conduct must therefore be easy to find and easy to use. The Code of Conduct shall provide a set of concrete and detailed guidelines for how companies comply with all or parts of the GDPR[31]. The companies must be able to find answers to practical industry-specific questions. The Codes of Conduct should therefore be designed as specific templates, recipes, procedures, solutions and / or processes that are described in a "familiar way" within the industry. The Codes of Conduct shall contribute to the companies achieving their goals at the same time as they fulfil statutory obligations within privacy. They must facilitate the work processes so that it is easy for the companies to carry out their tasks at the same time as they follow the law.

2.2 General benefits of a Code of Conduct

A well-written Code of Conduct might help controllers and processors reflect on processing activities and ensure that they follow rules designed for their sector to achieve best practice.

The development and the approval of Codes of Conduct are likely to deliver a number of benefits. A good Code of Conduct can provide guidance when establishing and updating best practice for compliance in specific processing contexts, as well as enabling data controllers and processors to commit to compliance with recognized standards and practices and be recognised for doing so[32]. In general, a Code of Conduct can make it easier to follow the GDPR.

[28] Op.cit., EDPB's Guidelines, chapter 5.2 and 5.8

[29] Op.cit., GDPR, Art. 5 (2) and 24

[30] Op.cit., GDPR, Art. 40 (1) and (2)

[31] Op.cit., EDPB`s Guidelines, chapter 3

[32] Op.cit., EDPB`s Guidelines, chapter 4

A Code of Conduct can provide a reduction of administrative burden of proving compliance, especially for small and medium-sized enterprises that do not have the capacity to familiarise themselves with the regulations in detail[33].

As well as setting rules to follow, the Code of Conduct can reduce the risk of sanctions (such as fines) and reputational loss. Joining a Code of Conduct can be a beneficial advantage since good privacy provides confidence.

Cooperation within the industry gives the individual enterprise the opportunity to participate in discussions and influence how the industry adapts to the GDPR and may result in companies receiving services beyond the actual Code of Conduct, such as guidance and assistance in privacy issues[34].

2.3 Why a SSH GDPR Code of Conduct can be beneficial for research

Assuming that legal texts are not always easily accessible and understandable, a SSH GDPR Codes of Conduct especially developed for research will be, in the task team's opinion, of great benefit. In the following section, the task team addresses some of the benefits identified for a SSH GDPR Code of Conduct for research purposes.

By using a common SSH GDPR Code of Conduct to create standards, the individual research institution might not need to spend time and resources on interpreting the law into industry-specific issues. The SSH GDPR Code of Conduct will clarify and specify certain rules of the GDPR for controllers who process personal data for purposes of scientific research35. This can be efficient and resource saving for the research sector and for the individual business and at the same time provide higher assurance, which in turn can contribute to greater support or higher response rate.

A SSH GDPR Code of Conduct can also result in higher confidence in the authorities, which can help maintain and develop research-friendly regulations. It can also be a reassurance for the research institutions to know that the procedure has been approved by the supervisory authority.

Similar practices across the research environment can also be an advantage in contact with both data subjects, partners, sponsors, and clients[36]. Common templates or standards simplify everyday life for researchers, including collection, storage, sharing and further use. This can also apply for EOSC. If

[33] Ibidem

[34] Ibidem

[35] Op.cit., GDPR, Art. 40(2)

[36] Op.cit., EDPB`s Guidelines, chapter 4

research data, for instance, has been collected based on the same template for information to participants, the same conditions can apply for storage and further use.

Furthermore, a SSH GDPR Code of Conduct can contribute to expedient research processes and innovation and help facilitate collaboration across companies within the same sector. When everyone uses the same standard, a good idea can be implemented more easily, which in turn facilitates the building of a safe, secure, sustainable, and profitable research community.

Common frameworks can facilitate the collection, long-term storage, sharing and further processing of personally identifiable research data across European countries.

It is important to remember that privacy (compliance) is not something researchers or research institution do in addition to the research, but as an integral part of the research process[37]. Privacy should be thought of as a means to an end. Privacy provides trust, and the research environment benefits from it.

SSH GDPR Codes of Conduct can contribute to research taking place within the framework of the regulations. The GDPR is general and applies to all processing of personal data[38]. A SSH GDPR Code of Conduct can explain how research can be carried out in accordance with this Regulation.

Common frameworks can facilitate the collection, long-term storage, sharing and further processing of personally identifiable research data across European countries, but adherence to SSH GDPR Codes of Conduct can also show that data controllers and data processors located outside the EU / EEA have implemented adequate safeguards in order to permit transfers under Article 46[39]. This can be considered desirable for research purposes, where cross border collaboration is encouraged. It is the understanding of the task team that transfers made based on an approved SSH GDPR Code of Conduct, together with binding and enforceable obligations of the collaborator to apply appropriate safeguards, may be possible without any prior approval from a supervisory authority. This can be an advantage for EOSC, as more data can be shared without being at the expense of previous consents or information in relation to data subjects (participants).

2.4 Possible consequences of not creating a SSH GDPR Code of Conduct

Reusing data created by others holds great promise in research. However, it is the task teams understanding that large amounts of research data collected in Europe today cannot be reused, to be

[37] Op.cit., GDPR, Art. 5 (2), Art. 24

[38] Op.cit., GDPR, Art. 1 and the following articles in Chapter 1

[39] Op.cit., GDPR, Art. 40(3)

processed in accordance with the GDPR and/or contracts with data subjects (participants). An important reason is the lack of a lawful basis for further processing of personal data.

The processing of personal data for research purposes is regulated by law, and the regulations are complicated[40]. Although the GDPR emphasises the importance of - and facilitates - research[41], it can be difficult to spot the scope of research in the regulations. It requires both competence and good planning e.g., a data management plan. In addition, different laws in the Member States[42] can make it difficult to share data across Europe. These factors contribute to inhibiting research to be carried out in a way that enables long-term storage and sharing/reuse of personal data in new research projects.

One primary goal in the EU's enactment of the GDPR was to harmonise, or bring into conformity with each other, the data protection laws of the EU/EEA Member States, in order to facilitate the "free flow" of personal data within a safe framework[43]. This harmonisation was also one of the main purposes for enacting the EU Data Protection Directive[44], which served as the source of EU data protection law prior to the GDPR. Privacy should maintain the same high standard throughout the EU and EEA, through a set of rules that give companies the same duties and citizens the same rights.

The GDPR aims to protect the privacy of citizens, and improve how personal data are collected, handled, processed, and stored[45]. It is a landmark in regulating use and misuse of private and sensitive data. In the field of research, the GDPR has opened for (and to some extent imposed) a large degree of national adaptations[46]. Although the Member States can't modify the GDPR, each of them needs national legislation to accompany it for two reasons. First, such legislation is needed for the GDPR to fit appropriately into the member state’s legal framework. National legislation is needed to select among the variations permitted in the GDPR itself. When the regulations vary between the European countries, it can provide different conditions for the processing of personal data in research. Thus, European research collaboration has its share of challenges. Different rules can make it difficult to collaborate on the storage and sharing of personal data for research purposes.

[40] Op.cit., GDPR, Art. 6 and 9

[41] Op.cit., GDPR, Art. 89

[42] Op.cit., GDPR, Art. 9 (4)

[43] What is GDPR, the EU’s new data protection law? Accessible at: https://gdpr.eu/what-is-gdpr/

[44] DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995, accessible at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&rid=5

[45] Op.cit., GDPR, chapter 1

[46] Op.cit., GDPR, Art. 89 (2)

At the same time, the GDPR encourages industry specific SSH GDPR Codes of Conduct[47]. A SSH GDPR Code of Conduct is a practical tool - in the form of providing common templates / standards - that will make it easier to follow the privacy regulations within a sector[48].

Research is one of the areas of society that can be particularly served by SSH GDPR Codes of Conduct, because different rules for research applies in different countries[49]. At the same time, the variation in the regulations contributes to the fact that research may also be one of the areas for which SSH GDPR Codes of Conduct are most challenging. There are several national adaptations to consider when planning a SSH GDPR Code of Conduct.

Nevertheless, without such SSH GDPR Codes of Conduct within the field of research, European cooperation can be demanding. It can be virtually impossible to collect large amounts of research data for long-term storage and sharing across European countries. Such a consequence will, in the task team`s opinion, not only be a loss for research, but also for the society.

3. Which terms must be fulfilled when creating a Code of Conduct?

3.1 Introduction

The GDPR article 40 and 41 establish the legal ground for the creation of SSH GDPR Code of Conducts[50]. These articles provide information on what a SSH GDPR Code of Conduct can regulate, and which procedural steps that must be taken to enable a SSH GDPR Code of Conduct to be approved. In Chapter 0 and 0 of this Deliverable, the task team presents suggestions on what a SSH GDPR Code of Conduct can regulate, and naturally to be included when developing the SSH GDPR draft Code of Conduct.

The procedural demands on how to create a SSH GDPR Code of Conduct created, can be divided into two, namely, first how to get a SSH GDPR draft Code of Conduct admissible, and two; how to get the final

[47] Op.cit., GDPR, Art. 40

[48] Op.cit., EDPB`s Guidelines, chapter 3

[49] Op.cit., GDPR, Art. 89 (2)

[50] Op.cit., GDPR, Art. 40 and 41

SSH GDPR Code of Conduct approved[51]. As this deliverable intend to start the initiative to enable the drafting of a SSH GDPR Code of Conduct, the focus will be to address terms for the first stage. This is intended to inspire the work in WP8, which can further plan how to fulfil the terms for drafting a Code of Conduct draft, and thereafter explore extended terms to get a Code approved once a draft is considered admissible.

The terms to be addressed are identified by interpretation of GDPR article 40 and 41[52], and by studying the guideline on Code of Conducts and monitoring bodies published by EDPB[53]. This guideline is meant to assist on how GDPR article 40 and 41 are to be practised[54]. The guideline also divides the process into two; how to get a SSH GDPR draft Code of Conduct admissible, and two; how to get the final SSH GDPR Code of Conduct approved[55]. This might indicate the importance of structuring the work into separate phases, and to make sure all terms are fulfilled in each phase. Phase 1 will be the precondition for starting phase 2. As this Deliverable intent to start the initiative, it will have focus on explaining "phase 1", as this will explain what needs to be further discussed in the upcoming work of WP8.

As the following shows, multiple procedural actions must be taken to enable a draft SSH GDPR Code of Conduct to be evaluated and considered admissible. The terms presented in 3.2 are set to enable an effective evaluation on any draft Code[56] , and will therefore be relevant for the further initiative to be taken within WP8.

3.2 Terms to get draft SSH GDPR Code of Conduct admissible

3.2.1 Who to represent the SSH Environment?

The GDPR article 40 (2) states that "associations and other bodies representing categories of controllers or processors may prepare Code of Conduct, or amend or extend such codes"[57], for the purpose of

[51] Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, accessible at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-0_en

[52] Op.cit., GDPR Art. 40 and 41

[53] Op.cit., Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679

[54] Op.cit., EDPB's Guidelines, section 3

[55] Op.cit., EDPB's Guidelines, chapter 5 and 6

[56] Op.cit., EDPB`s Guidelines, section 19

[57] Op.cit., GDPR Art. 40(2)

specifying the application of GDPR. The categories of controllers or processors can be named as "code owners"[58].

Therefore, the wording in GDPR art. 40(2) states that the body drafting the SSH GDPR Code of Conduct must be able to represent the SSH research environment. Based on the wording, several representatives can perform this task in collaboration, presumed each are able to represent the SSH environment. The representatives must be able to demonstrate that they understand the SSH Environment and to define which activities and sector the SSH GDPR Code of Conduct covers.

As the task of initiating a SSH GDPR Code of Conduct has been assigned to Task 5.3 and 8.3, this can indicate that the involved bodies are considered appropriate to represent the SSH environment. However, this must be determined on a concrete documented assessment, as the outcome of who is the representative body must be argued in the SSH GDPR Code of Conduct draft[59].

According to EDPB`s guidelines, the representatives can be identified by "number or percentage of potential code members" from the SSH Environment and "Experience of the representative body regarding the sector and processing activities concerning the code"[60].

3.2.2 Explanatory statement and supporting documents

According to EDPBs guidelines, all Code of Conduct drafts must contain specific explanatory statements[61]. This statement must contain information on the scope of the Code of Conduct being drafted, the purpose and how it plans to facilitate the effective application of GDPR. The draft must also be supported by documents, to demonstrate the need for a SSH GDPR Code of Conduct[62].

The finding Task 5.3`s deliverable`s, 5.7, 5.19 and 5.8 might be used to supporting documenting the need of creating a SSH GDPR Code of Conduct. However, the further initiative within WP8 should gather additional documentation to underline the need for a SSH GDPR Code of Conduct. This might for instance be done, in the task team`s opinion, by conducting interviews with the environment, holding Workshops and/or surveys within the SSH environment etc.

The need for such a documentation also highlights the importance of including the SSH environment in the further initiative. The ones who should be contacted, must also be further explored. In this

[58] Op.cit., EDPB`s Guidelines, section 21

[59] Op.cit., EDPB`s Guidelines, section 22

[60] Op.cit., EDPB`s Guidelines, section 21

[61] Op.cit., EDPB`s Guidelines, section 20

[62] Ibidem

Deliverable, in Chapter 0, the task team presents an analysis that can be further developed and used for this purpose.

3.2.3 Processing and territorial scope of the SSH GDPR Code of Conduct

The SSH GDPR Code of Conduct draft must, according to EDPB, have "a defined scope that clearly and precisely determines the processing operations (or characteristics of the processing) of personal data covered by it, as well as the categories of controllers or processors it governs. This will include the processing issues that the code seeks to address and provide practical solutions"[63].

As mentioned in the beginning of this Deliverable, the term "processing" means all operations or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as gathering, storage, recording, making available, analysing, transferring of personal data[64] Further, the term "personal data" means all data related to an identified or identifiable person65 ("data subject"). This can include directly identifiable data, such as names or mail addresses, or indirectly, by combining variables or usage of a scrambling key. It can also include processing of pseudonymised data, meaning data not containing indirectly of directly identifiable variables, but linked to a scrambling key, reidentification it possible[66].

This indicates that the further initiative must address the scope of the SSH GDPR Code of Conduct, considering all the different processing operations within the SSH environment (storing, gathering, analysing, making available research data etc.). It should also address if it applies to the SSH environment in general, or for parts of the environment. The defined SSH processing scope and who the Code if meant to apply for within the SSH environment, should be able to specify which issues the SSH GDPR Code of Conduct wish to reflect and resolve[67].

The SSH GDPR Code of Conduct draft code must also define to where it applies, in only in one country or across borders[68]. In the task team`s opinion, it is naturally to conclude that a SSH GDPR Code of Conduct to be initiated through a Deliverable within SSHOC, will be defined as an international Code of Conduct (within Europe).

3.2.4 Supervisory authority

[63] Op.cit., EDPB`s Guidelines, section 23 and 24
[64] Op.cit., GDPR, Art. 4 (2)
[65] Op.cit., GDPR, Art. 4 (1)
[66] Op.cit., GDPR, Art. 4 (5)
[67] Op.cit., EDPB`s Guidelines, Section 23 and 24
[68] Ibidem

All Code of Conduct drafts must be submitted to and assessed by a supervisory authority[69]. All EU/EEA countries are obliged to provide an independent public authority responsible for monitoring the application of the GDPR[70]. The supervisory authorities must be competent to perform the task it has been assigned, including mandate and power set in GDPR[71]. The upcoming work within WP8 should include an assessment of which supervisory authorities are competent to assess a SSH GDPR Code of Conduct draft.

The supervisory authority receiving the SSH GDPR Code of Conduct draft must be competent to review the draft and the owner of the code is responsible for identifying the competent supervisory authority[72]. If the territorial scope of the Code is national, the competent supervisory authority to assess the draft will be the supervisory authority within that country[73].

However, if the Code of Conduct will have an international scope, the code owners must perform a broader assessment to determine the applicable competent supervisory authority[74]. This implies that the upcoming work should include an assessment of which supervisory authority are competent to assess a SSH GDPR Code of Conduct draft, as all supervisory authorities are to receive a version of the draft in the language being used in that country, as well as an English version[75].

EDPB has in its guideline presented a list of non-exhaustive factors, to assist code owners determine which supervisory authority is appropriate for the specific Code of Conduct draft. The factors to be considered are:

- "The location of the largest density of the processing activity or sector.
- The location of the largest density of data subjects affected by the processing activity or sector.
- The location of the code owner`s headquarters.
- The location of the proposed monitoring body`s headquarters or
- The initiatives developed by a supervisory authority in a specific field"[76].

3.2.5 Determine mechanisms

[69] Op.cit., GDPR, Art. 40 (5)
[70] Op.cit., GDPR, Art. 51(1)
[71] Op.cit., GDPR, Art. 55 (1)
[72] Op.cit., EDPB`s Guidelines, section 25
[73] Op.cit., GDPR Recital 122
[74] Op.cit., EDPB`s Guidelines, Appendix 2
[75] Op.cit., GDPR, section 30
[76] Op.cit., GDPR, Appendix 2

The GDPR article 40 (4) states that a Code of Conduct "...shall contain mechanisms which enable the body referred to in Article 41 (1) to carry out the mandatory monitoring of compliance with its provisions by the controller or processors which undertake to apply it..."[77].

Therefore, the SSH GDPR Code of Conduct draft must include a plan for mechanisms to enable the monitoring of the SSH GDPR Code of Conduct`s. This means that a monitoring body for a SSH GDPR Code of Conduct also must be identified, see section 3.2.6 of this Deliverable.

3.2.6 Identify a Monitoring body

The SSH GDPR Code of Conduct draft must, in accordance with the guidelines presented by EDBP, "...identify a monitoring body and contain mechanisms which enable that body to carry out its function as per Article 41 of the GDPR"[78]

Therefore, the further initiative to be taken within WP8 should include an assessment of which monitoring body would be appropriate for a SSH GDPR Code of Conduct. Further, it must be addressed which mechanisms will enable the identified monitoring body to perform its tasks.

The Monitoring body must, in accordance with GDPR article 41 (1)[79], have an appropriate level of experience in relation to the subject matter of the SSH GDPR Code of Conduct and must be accredited for this concrete purpose by the competent supervisory authority.

Within GDPR article 41 (2)[80] terms are set to enable a supervisory authority to accredit a Monitoring body. A monitoring body can be accredited to monitor compliance with a SSH GDPR Code of Conduct, if the body has:

"(a) demonstrated its independence and expertise in relation to the subject-matter of the code to the satisfaction of the competent supervisory authority.

(b) established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operations.

[77] Op.cit., GDPR Art. 40(4)

[78] Op.cit., EDPB's Guidelines, section 27

[79] Op.cit., GDPR, Art. 41(1)

[80] Op.cit., GDPR, Art. 41(2)

(c) established procedures and structures to handle complaints about infringements of the code or the way the code has been, or is being, implemented by a controller or processor, and to make those procedures and structures transparent to data subjects and the public; and

(d) demonstrated to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interest."[81]

The body to monitor a SSH GPDR Code of Conduct must therefore be independent and experienced within the SSH environment. Identifying this body will be essential for further work on initiating the Code of Conduct, as information about the body and how it can monitor the Code of Conduct must be included in a draft to be admissible by the competent supervisory authority[82]. As the monitoring body must be accredited by the competent supervisory authority[83], it also reflects on the importance of identifying the competent supervisory authority.

When discussing who is applicable for monitoring, the task team encourages the further initiative to gather inspiration from the experiences of BBMRI-ERIC`s, working on a health and life Science GDPR Code of Conduct.

3.2.7 Consult with stakeholders

Recital 99 of the GDPR states that when drawing, extending, or amending a Code of Conduct, relevant stakeholders, including data subjects, should be consulted, confirming, and demonstrating that a appropriate level of consultation has been performed[84]. The SSH GDPR Code of Conduct draft must contain information as to the extent of such consultations performed[85]. If no consultation has been performed, the code owner must be able to explain why[86]. It is the task team`s opinion that such consultation within the SSH environment, should be planned and performed at an early stage in the further work on creating a SSH GDPR Code of Conduct draft. Who to consult with is likely to be affected by the scope of the SSH GDPR Code of Conduct draft (see section 3.2.3 of this deliverable).

According to EDPB, the draft can include "...information about other codes of conducts that potential code members may be subject to and reflect how their code complements other codes. This should also

[81] Ibidem

[82] Op.cit., EDPB`s Guidelines, section 26 and 27

[83] Op.cit., GDPR, Art. 41(1)

[84] Op.cit., GDPR, Recital 99

[85] Op.cit., EDPB's Guidelines, section 28

[86] Ibidem

outline the level and nature of consultation which took place with their members, other stakeholders and data subjects or associations/bodies representing them"[87].

The EDPB recommends consulting with the members of the code owner and considering their relevant processing activities[88].

For the further work on initiating a SSH GDPR Code of Conduct, relevant stakeholders should therefore be identified. The task team has in this Deliverable started the work on performing a Stakeholder analysis, which can be further developed in WP8. This analysis is presented in Chapter 0 of this Deliverable. Note that this must be further developed, and a plan for how this should be actioned can be made in the further work in WP8.

3.2.8 Compliance with national legislation

The SSH GDPR Code of Conduct draft must be in compliance with relevant national legislation[89]. According to EDPB this applies, in particular," ...where the code involves a sector which is governed by specific provisions set out in national law or it concerns processing operations that have to be assessed, taking into account specific requirements and relevant legal obligations under national law"[90].

Considering that the GDPR provides Member States with the possibility to provide supplementary regulations related to research[91], this will be important to keep in mind when drafting a SSH GDPR Code of Conduct.

As the SSH GDPR Code of Conduct is likely to be international, such confirmation will prerequisite knowledge of national legislation in all relevant countries. In the further work, it will therefore be important to structure and prepare a plan on how this can be assessed and determined.

3.2.9 The language of the SSH GDPR Code of Conduct draft

The language of the SSH GDPR Code of Conduct will be reliant on the determination on which supervisory authorities are competent to review the draft[92].

[87] Ibidem

[88] Ibidem

[89] Op.cit., EDPB's Guidelines, section 29

[90] Ibidem

[91] Op.cit., GDPR, Art. 89(2)

[92] Op.cit., EDPB`s Guidelines, section 30

As mentioned, the supervisory authority receiving the draft Code must be competent to review the draft and the owner of the code is responsible for identifying the competent supervisory authority[93]. If the territorial scope of the Code is national, the competent supervisory authority to assess the draft will be the supervisory authority within the country[94]. Then the code draft should be written in the applicable language used in that specific country, as well as English[95].

However, as mentioned, if the Code will have an international scope, the code owners must perform a broader assessment to determine the applicable competent supervisory authority[96]. This should be encouraged to be assessed in the beginning of planning the draft to be written, as all supervisory authorities should receive a version of the draft in the language being used in that country, as well as an English version[97]. Therefore, which languages the SSH GDPR Code of Conduct draft should be written in, will depend on the assessment of which supervisory authorities are competent.

As the SSH GDPR Code of Conduct, in the task team`s point of view, is likely to be international, several supervisory authorities within Europe might be competent to review the draft. Particular supervisor authority, in terms of competence affecting particular language, must be presented in the draft and might be determined by using the list of non-exhaustive factors presented in section 3.2.4 of this deliverable.

4. What can a SSH GDPR Code of Conduct contain?

4.1 Introduction

The GDPR article 40 and 41[98] establish the legal ground for the creation of Code of Conducts. The articles provide information on what a Code of Conduct can regulate, and which procedural steps that must be taken to enable a Code of Conduct to be approved. In Chapter 3 of this Deliverable, the terms/procedural steps on how to create a SSH GDPR Code of Conduct was presented. In the current chapter of this Deliverable, the task team presents suggestions on what a SSH GDPR Code of Conduct can regulate.

[93] Op.cit., EDPB`s Guidelines, section 25
[94] Op.cit., GDPR, Recital 122
[95] Op.cit., EDPB`s Guidelines, section 30
[96] Op.cit., EDPB`s Guidelines, Appendix 2
[97] Op.cit., EDPB`s Guidelines, section 30
[98] Op.cit., GDPR, Art. 40 and 41

4.2 A broad or narrow scope of a SSH GDPR Code of Conduct?

When developing a Code of Conduct, there are a wide framework for themes or topics[99]. One possible approach might be to introduce a comprehensive Code of Conduct that addresses many of the articles in the GDPR. The Code of Conduct could start with a large common framework that provides standards and tools for the entire research process within all branches of humanities and social science research. Such a broad Code of Conduct could be presented as a reference work where researchers and research institutions can find templates for relevant documents and data, e.g., different types of data collection, and analyses, to the storage, sharing and anonymization of personal data within a wide range of research methods.

This could be a framework consisting of guidelines for how research be performed according to the privacy principles within GDPR[100], find a lawful basis in GDPR[101], safeguard the rights of data subjects within GDPR[102], how the research institutions can ensure internal control regulated in GDPR[103], and built-in privacy regulated in GDPR[104]. Further, it could concern how to ensure information security and follow up on discrepancies as regulated in GDPR[105] , how to ensure good agreements with partners (joint data controllers and data processors)[106], how and when to carry out data protection impact assessments (DPIA) [107] and prior consultations in accordance with GDPR [108] , how to facilitate Data Protection Official/Officer[109], and ensure legal transfers to third countries in accordance with GDPR[110].

The advantages of such a broad SSH GDPR Code of Conduct can be that researchers and research institutions get a large reference work gathered in one place, which may provide answers to many practical questions and solves a wide range of issues related to privacy in research, within different branches of social research. This can make it easier for researchers and research institutions to demonstrate compliance with data protection principles[111]. The disadvantage will be the enormous

[99] Op.cit., GDPR, Art. 40 (2)
[100] Op.cit., GDPR, Art. 5
[101] Op.cit., GDPR, Art. 6 and 9
[102] Op.cit., GDPR, Art. 12 to 22
[103] Op.cit., GDPR, Art. 24
[104] Op.cit., GDPR, Art. 25
[105] Op.cit., GDPR, Art. 32 to 34
[106] Op.cit., GDPR, Art. 26 and 28
[107] Op.cit., GDPR, Art. 35
[108] Op.cit., GDPR, Art. 35 to 36
[109] Op.cit., GDPR, Art. 37 to 39
[110] Op.cit., GDPR, Chapter 5
[111] Op.cit., EDPB`s Guidelines, section 12

amount of work required to complete and draft such a Code of Conduct. The risk of spending large amount resources on something that may prove difficult to concretize.

Another possibility may be to narrow the scope of the SSH GDPR Code of Conduct, and instead focus on one or two practical aids that could be beneficial for research. This can include preparing specific templates for obtaining a lawful basis for the processing of personal data collected from the data subject. Examples of such templates can include:

- A template for information letters for "broad consent", long-term storage, and sharing of research data within the SSH environment
- A checklist of measures that can safeguard the data subject's rights and freedoms, as an aid in determining the lawful basis in GDPR article 6(1) letter e[112]
- A tool for safeguarding the rights of research participants
- A Code of Conduct for information security in research
- A standard for conducting DPIAs and prior consultations in research

The advantage of a narrow SSH GDPR Code of Conduct is, in the opinion of the task team, that it might be easier to implement. With good planning and adapted resources, it can be realistic to have a tangible result prepared, and thereby providing a practical tool that research can benefit from in a relatively short time. The disadvantage, in the opinion of the task team, is that the SSH GDPR Code of Conduct will only be helpful in a limited part of the research (e.g., only for research that is in contact with the data subjects). However, by making strategic choices for the scope of focus, a narrow SSH GDPR Code of Conduct can be of great help and can become an effective contribution to long-term storage and sharing of research data in Europe.

In addition, if creating a narrow SSH GDPR Code of Conduct, it might be possible to expand to a broader SSH GDPR Code of Conduct or a more comprehensive reference work[113].

[112] Op.cit., GDPR Art. 6 (1)

[113] Op.cit., GDPR art. 40(2) wording indicating the possibility of extending codes

5. Proposing a Code of Conduct for SSH

5.1 Introduction

The Deliverable will in Chapter 5 provide some suggestions for what a SSH GDPR Code of Conduct draft may regulate, leaning among others on results from Deliverable 5.7 and 5.19. However, it is important to highlight that some of the terms/procedural steps identified in Chapter 0 of this Deliverable, can affect what the draft can contain. As a plan must be made on how to fulfil these terms, and this deliverable does not present a first version of a SSH GDPR Code of Conduct draft. When and how the SSH GDPR Code of Conduct draft should be written, must be further elaborated in WP8, Task 8.3. The same applies for deciding the content of the code draft.

As presented in Chapter 4 of this Deliverable, several issues may be regulated within a SSH GDPR Code of Conduct. The final scope and issue to be regulated should be jointly decided by the SSH environment, represented by key Stakeholders, to make sure the issues can represent the sector.

The task team recommends the establishment of a SSH GDPR Code of Conduct concerning the lawful basis of processing of personal data for research purposes[114].

First, the task team will explain what is meant by a lawful basis, and which lawful bases are the most relevant for research. Second, the task team will see what advantages and disadvantages the various lawful bases can have for research (and European research collaboration). And last, the task team will argue why it think it will be beneficial to establish a common SSH GDPR Code of Conduct concerning lawful bases for processing in research.

5.2 What is a lawful basis, which lawful bases are the most relevant for research, and which conditions apply?

All processing of personal data must fulfil the conditions in at least one of the alternatives in the GDPR Article 6 (1)[115]. The party responsible for the processing of personal data (data controller) must in advance

[l14] Op.cit., GDPR, Art. 6 and 9

[115] Op.cit., GDPR, Art. 6(1)

determine what the lawful basis for the processing is and ensure that the conditions are met[116]. If not, the processing of personal data will be unlawful[117].

When processing personal data in research, it is most common to refer to GDPR lawful bases Art. 6(1) letter a, which states that "the data subject has given consent to the processing of his or her personal data for one or more specific purposes;"[118] or GDPR Art. 6(1) letter e, stating "processing is necessary for the performance of a task carried out in the public interest (...)"[119].

The GDPR's Art 6(1) letter f[120] can also be an alternative. A condition in this provision is that the "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child"[121].

The processing of special categories of personal data is more strictly regulated than general categories of personal data[122]. Special categories of personal data refer to racial or ethnic origin, political opinions, religious beliefs, philosophical beliefs, Trade Union Membership, genetic and biometric data processed with the unequivocal purpose of identifying a natural person, health data, or information about a natural person's sex life or sexual orientation[123]. The processing of such personal data is by default unlawful[124]. In order to be lawful, the processing must be rooted in one of the exemptions in Art. 9(2) letter a to j[125], in addition to have a lawful basis in Art. 6(1)[126].

When special categories of personal data are processed for research purposes, it is common to refer to the exemption in the GDPR Art. 9(2) letter a, letter j or letter e[127].

[116] Op.cit., GDPR, Art. 5 (2) and 24

[117] Op.cit., GDPR, Art. 6(1) and 9(2)

[118] Op.cit., GDPR, Art. 6(1) letter a

[119] Op.cit., GDPR, Art. 6(1) letter e

[120] Op.cit., GDPR, Art. 6(1) letter f

[121] Ibidem

[122] Op.cit., GDPR, Art. 6 and 9

[123] Op.cit., GDPR, Art. 9(1)

[124] Ibidem

[125] Op.cit., GDPR, Art. 9(2)

[126] Op.cit., GDPR, Art. 6(1)

[127] Op.cit., GDPR, Art. 9(2) letter a, letter j and letter e

The GDPR art. 9(2) letter a, states that processing is lawful if "the data subject has given explicit consent to the processing of those personal data for one or more specified purposes (…)"[128]. Further, the GDPR Art. 9(2) letter j provides a lawful basis if "processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject"[129]. Further, GDPR Art. 9(2) letter e, can be used as a lawful basis when it is processed personal data which are "manifestly made public by the data subject"[130]. Other lawful bases found in GDPR Art. 9(2)[131] can also be relevant in research, however, it is the assumption of the task team that the three lawful bases mentioned above are the most common used for research purposes. These will therefore not be mentioned further in this Deliverable.

For the lawful bases Art. 6(1) letter e and Art. 9(2) letter j, the GDPR Art. 6(3) demands that Union or Member State law determines supplementary lawful basis. In the supplementary lawful basis, the Member States can conclude on their own conditions and will apply in addition to the general conditions in the GDPR. The GDPR's Art. 9(4) states that "Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health." This implies that the Member States can adopt stricter rules concerning the processing of these types of special categories of personal data, than what is generally required in the GDPR. There can therefore be large national variations in which conditions applies to the processing when researching such types of personal data.

The processing of personal data relating to criminal convictions and offences can only be carried out under the control of a public authority, or if such processing is authorized by Union or Member State law[132]. This implies that it is only allowed to research on such types of personal data if there is a lawful basis for the processing in national law (as long as Union law has not authorized it)[133]. The Member States can also in this context determine special conditions for the processing, as the GDPR ensures that the lawful basis shall guarantee the "fundamental rights and freedoms of the data subject"[134]. This implies again that there might be large national variations in what conditions applies for the processing. A shared condition, however, is that comprehensive registries of criminal convictions can only be done under the

[128] Op.cit., GDPR, Art. 9(2) letter a

[129] Op.cit., GDPR, Art. 9(2) letter j

[130] Op.cit., GDPR, Art. 8(2) letter e

[131] Op.cit., GDPR, Art. 9(2) letter a – j

[132] Op.cit., GDPR, Art. 10

[133] Ibidem

[134] Ibidem

control of national authorities[135]. It is the understanding of the task team that this provision[136] has limitations as for how large registries of criminal convictions that can be made available/utilized for research purposes.

5.3 Advantages and disadvantages of different lawful bases for processing personal data

5.3.1 Consent

As mentioned in Chapter 5.1 in this Deliverable, all processing of personal data must fulfil the conditions in at least one of the alternatives in the GDPR Article 6 (1). Consent is one of the lawful bases that is widely used in research. For a consent to be valid, several conditions within GDPR must be met. The GDPR art. 4(11) defines consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". Further, the GDPR Art. 7 states that the GDPR also requires that the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data and that the data subject shall have the right to withdraw his or her consent at any time.

In some research projects, it may be both possible and desirable to take measures to ensure that the processing of personal data can be based on consent. It can e.g., apply to research where the data subject[137] actively contributes to the data collection through interviews, questionnaires, or participatory observation. Consent may also be relevant for data collection from journals and registers, or from occupational groups that have a duty of confidentiality, by asking the data subject to allow confidential personal data to be used in research. In other research projects, however, it can be impossible to meet the consent requirements, because it will make it disproportionately difficult or impossible to achieve the research purpose. Hence, consent cannot be regarded as a silver bullet when it comes to the processing of personal data within research.

Whether consent will be an alternative for a concrete processing activity, can e.g., depend on the nature, purpose, methods, data sources, and sample of the research. In section 0 of this deliverable, the focus will be on the various conditions for consent followed by an explanation of why those can be difficult to

[135] Ibidem

[136] Ibidem

[137] Op.cit., GDPR, Art. 4(1)

fulfil in some contexts. In research, it is not always easy to meet all these requirements. Hence, consent is not always considered as an appropriate lawful basis.

5.3.1.1 The consent must be freely given

The requirement for freely given consent essentially means that the data subject willingly consents to the processing of personal data[138]. As stated in Recital 43 of the GDPR "consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment". The data subject shall not experience any pressure to disclose the information[139]. As a rule, the GDPR prescribes that if the data subject has no real choice, feels compelled to consent or will endure negative consequences if they do not consent, then consent will not be valid[140]. Also, the data subject must be able to understand that the processing of personal data is voluntary.

If the data subjects possess consent competence or capacity, and are actively participating in research, it would be contrary to ethical standards not to facilitate volunteering, regardless of the lawful basis. Thus, the condition of freely given consent is normally not an obstacle to using consent as a lawful basis in such contexts. For research involving vulnerable people, on the other hand, it is more complicated to ensure that participation is voluntary. Individuals can be vulnerable where circumstances may restrict their ability to freely consent or object to the processing of their personal data, or to understand its implications. In such research contexts, it may be difficult to ensure that the consent is freely given.

I some cases it may be appropriate to carry out the research, following a specific legal and ethical assessment in which the benefit of the research is weighed against the disadvantages for the participants, and appropriate measures are introduced to safeguard the data subject. Nevertheless, these measures will not always be sufficient to ensure that voluntary participation is safeguarded in such a way that consent can constitute the lawful basis for the processing of personal data. In such cases, it would be more appropriate to find another legal basis for the processing.

5.3.1.2 The consent must be specific

According to GDPR article 7, "the request for consent shall be presented in a manner which is clearly distinguishable from the other matters".

[138] Op.cit., GDPR, Art. 4(11)

[139] Ibidem

[140] Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent, p. 12, accessible at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf

This entails that it should be clear what data processing activities will be carried out, granting the data subject an opportunity to understand and consent to each activity. If there are more than one reason to conduct a data processing activity, consent must be obtained for all purposes[141].

Regarding special categories of personal data as referred to in GDPR art. 9(1)[142], the data subject must explicitly consent to processing for one or more specific purposes to be in accordance with GDPR article 9(2) letter a.

5.3.1.3 The consent must be informed

Prior to obtaining consent, it is essential that the data subject have received useful information regarding what the processing of personal data entails, so that they are able to make informed decisions and understand what they are agreeing to[143]. It is an underlying premise here that the person in question is able to understand the information. Consent should only be used as a lawful basis when the data subject has the cognitive capacity to give an informed consent.

The requirement that the consent must be informed, must be interpreted in the light of the principle of fairness and transparency presented in GPPR article 5. As a minimum, the data subject must have received information about who is responsible for processing, what the purpose is, what data is to be processed, the right to withdraw consent, and (where applicable) the risk of transfer to a third country[144].

The requirement for informed consent should also be interpreted considering the responsibility of the data controller to facilitate that the data subjects can exercise their rights under the GDPR, including the right to information. The GDPR Articles 12 to 14 sets requirements for the form, content, and time of the information to be provided to data subjects.

The formal requirement is that information must be provided in a concise, open, comprehensible, and easily accessible manner, and in a clear and simple language. To ensure an open and fair processing of personal data, there are also several content requirements for the information. It is the understanding of the task team that the information must enable the data subject to understand what the processing entails, so that the person in question can assess the risk himself/herself. The registered person shall also be enabled to contact the data controller and his or her privacy representative, in order to obtain

[141] GDPR, consent must be specific, accessible at: https://gdpr.eu/gdpr-consent-requirements/

[142] Op.cit., GDPR, Art. 9(1)

[143] Op.cit., GDPR, Art. 4(11)

[144] Op.cit., GDPR, Third Countries

more information about the processing and exercise their rights, e.g., for inspection, correction, deletion[145].

In terms of time, the data subject must receive the information no later than at the start of the processing in research projects where the data subject himself provides personal data[146]. When the research collects personal information from others than the data subject, the requirement is that the data subject receives the information within a reasonable time (no later than 1 month) after collection, or (if applicable) at the time of contact with the data subject[147].

5.3.1.4 The consent must be unambiguous

Unambiguous consent means that the data subject gives consent through an active action that cannot be misunderstood. There should be no question about whether the data subject has consented for the processing of his or her personal data. In the processing of special categories of personal data, the requirement is stricter, in that the consent must be explicit[148], i.e., that it must be given in an extra clear manner.

5.3.1.5 The consent must be documented

Consent may be given orally, in writing or in another suited manner. The GDPR does not set out any formal requirements for consent. However, the data controller must be able to document that the consent exists. The GDPR clearly outlines the explicit obligation of the controller to demonstrate the consent of the data subject. The burden of proof will be on the controller[149].

The Recital of GDPR, section 42 states: "Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation". The consent may be presented in many ways, such as written declaration of consent or by an oral consent, which is documented on an audio / film recording. A data controller may also obtain explicit consent from the data subject by offering an explicit consent screen that contains 'Yes' and 'No' check boxes, on condition that that the text clearly indicates the consent.

In some cases, it will not be necessary for the research purpose to register personal data. Then documentation of consent may be contrary to the principle of data minimisation set in GDPR article 5. In these cases, it will be a discretionary assessment whether the consideration of data minimisation or the

[145] Op.cit., GDPR, Art 13

[146] Op.cit., GDPR, Art. 13(1)

[147] Op.cit., GDPR, Art. 14(3)

[148] Op.cit., GDPR, Art. 9(2) letter a

[149] Op.cit., GDPR, Art. 7 and 24

consideration of the data subject's co-determination (and control over the information) should be decisive. In the opinion of the task team, the assessment will i.e., depend on the type and extent of personal data that is processed, the purposes and the risk a personal data breach.

For some research projects, it is especially important to protect the identity of the participants. In these cases, the duty of the researcher – both legally and ethically – is to protect the participants by not registering direct personal information, because it can be dangerous for the participants if the information is misplaced. In other cases, the privacy consequences may not be that severe, but the participants may still refuse to give their names in a consent form. It can e.g., apply to research among illiterate / non-written societies, research on self-incriminating personal data, and research where the participants for other reasons are sceptical / have low confidence in the authorities / researchers. In such cases, the documentation requirement is an obstacle to using consent as a lawful basis. The solution can be to obtain ethical consent, but legally refers to another lawful basis for the processing of personal data, such as the GDPR article 6(1) letter e and article 9(2) letter j.

5.1.3.6 The right to withdraw consent

Under the GDPR article 13, a data subject must be informed about (among others) the identity and contact details of the data controller, the data protection officer, the purposes for which the data will be processed, the recipients of the data, the duration of storage and the right to withdraw consent if consent is the lawful basis of processing.

Allied with this extensive right to information, are the provisions on the right to withdraw consent and the obligation to inform data subjects about this right, and a key requirement is that consent must be as easy to withdraw as to give[150]. In some contexts, it can be difficult to facilitate the withdrawal of consent in research. This will perceptibly apply for cases where the research only processes indirectly identifiable personal data[151]. In many cases, data subjects may be difficult to identify in the data material, hence making it difficult to know with certainty that the data belongs to the given data subject.

[150] Op.cit., GDPR, Art. 4(11), 7 and 12

[151] Op.cit., GDPR, Art.4(1)

In addition, it may also be an obstacle to the research purpose if data subjects withdraw after their data has been included in analyses and scientific publications. In research with few registrants, withdrawal could destroy the entire research project. In research with many data subjects, it could affect the validity of the research results if there are biases in the sample groups that withdraw.

5.3.2 The processing is necessary for the performance of a task carried out in the public interest/scientific purposes

For the GDPR art. 6(1) letter e to be used as a lawful basis it is, as mentioned above, a condition that the "processing is necessary for the performance of a task carried out in the public interest (...)". For the use of GDPR's art. 9(2) letter j as a lawful basis when processing special categories of personal data, the processing must be considered necessary for research- or archiving purposes. Additionally, the processing must be in line with art. 89(1), and there must be a supplementary lawful basis in, for example Member State law, that determine additional safeguards for the processing. Common for all the conditions in the overall lawful basis, is that they must provide sufficient protection of the data subject's rights and freedoms.

An advantage with the lawful bases GDPR Art. 6(1) letter e, and Art. 9(2) letter j is that they give research quite flexible terms. The GDPR's art. 6(1) letter e and art. 9(2) letter j allow the data controller to a greater degree to adapt the data protection measures to the research context if the collective measures provide a sufficient safeguard of the fundamental rights and the interests of the data subjects.

A disadvantage with the lawful bases GDPR Art. 6(1) letter e, and Art. 9(2) letter j, is that it is challenging to gain oversight over all the applicable data protection measures. The research institutions could therefore put a collective overview (list) over such measures to good use. It can also be difficult to assess how the various measures should be combined in each processing in order for the safeguard about necessary guarantees to be upheld. This will require a case-by-case assessment in which the data controller must conduct and document. The demand is that the collective measures provide a sufficient safeguard of the data subject's rights and freedoms.

Another disadvantage that is just as challenging, particularly for research projects where personal data is processed across European countries, is the fact that there is a great variety in which measures the national supplementary lawful bases defines as necessary guarantees.

The GDPR art. 6(3) demands that the supplementary lawful basis to art. 6(1) letter e must ascertain the purpose of the processing. This enables the Member States to adopt specific provisions for the processing. Supplementary lawful bases to art. 9(2) letter j must be in accordance with art. 89(1), and "shall be proportionate to the aim pursued", "and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject".

This implies that the Member States can select various measures to protect the data subjects. These are set up as conditions for the processing of both general and special categories of personal data, according to GDPR art. 6(1) letter e and art. 9(2) letter j. The same will apply for personal data about criminal convictions and offences. That is, if the Member state allows these types of personal data to be used in research at all. In addition, concerning genetic data, biometric data, and health data, the Member States can introduce limitations[152] ensuring that the processing has stricter conditions than what is stated in the general rules of the GDPR. It is probable that national laws increasingly introduce such limitations for processing not based on consent. This can, amongst other things, apply to research on these types of personal data based on the GDPR's art. 6(1) letter e and art. 9(2) letter j.

For research on personal data based on art. 6(1) letter e and art. 9(2) letter j, there will consequentially be large national variations in what conditions applies for the processing. This applies particularly for research on health data, and genetic and biometric data. This lawful basis can as a result be problematic when personal data is processed across European countries.

For research on personal data only occurring within one country, however, it will be easier to use GDPR art. 6(1) letter e and 9(2) letter j as a lawful basis. In such cases, it is sufficient to follow the conditions provided in the country's laws. Where appropriate, the lawful basis can give research more flexible terms than consent. As shown above, there are several scenarios in which the conditions for consent can be difficult to meet in research.

5.3.3 Legitimate interests

GDPR Art. 6(1) letter f can be considered as the most flexible lawful basis for processing, but one cannot assume it will always be the most appropriate (ICO).

To use legitimate interest as lawful basis, the data controller must first be able to identify the interests and conduct a legitimate interest's assessment, to justify the decision of processing. It is the understanding of the task team that the controller must be able to demonstrate that its own interests are legitimate[153]. Thus, if a research institution chooses to rely on legitimate interest as lawful basis for processing personal data for scientific purposes, the institution must also be able to demonstrate that the research is in fact a legitimate interest.

Secondly, the data controller is committed to perform a balance test, demonstrating that the interests (i.e., rights and freedoms) of the data subject are not overriding the controllers' legitimate interests. The controller is then taking on extra responsibility for considering and protecting people's rights and interests[154].

[152] Op.cit., GDPR, Art. 9(4)

[153] Op.cit., GDPR, Art. 6 letter e and Art. 24

[154] IOC about Legitimate interests, accessible at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/

It is the opinion of the task team that it may be safer for research institutions to use GDPR Art. 6(1) letter e as lawful basis for processing of personal data for scientific purposes, pointing out that they are performing a public task. When using GDPR Art. 6(1) letter e the data controller will admittedly have to do a somewhat similar assessment as in GDPR Art. 6(1) letter f, arguing that the processing necessary for scientific purposes also gives appropriate protection of the interests of the registered. The advantage by using GDPR Art. 6(1) letter e, though, is that many national regulations define research as a public task, so the research institution may not have to demonstrate that research is a legitimate interest. GDPR Art. 9(2) letter j, which implicitly defines research as a task in public interest that legalize processing (under some conditions) is often used together with GDPR Art. 6(1) letter e as a lawful basis, when processing special categories of personal data for scientific purposes. Also, GDPR Art. 6(1) letter e with supplementary regulations, provide the research institutions with guidelines on what types of measures that can or must be used in the processing to give necessary guarantees for the rights and freedoms of the registered.

5.3.4 Data which are manifestly made public by the data subject

The processing of personal data for research purposes is permitted, according to GDPR article 9(2) letter e, if the "processing relates to personal data which are manifestly made public by the data subject ". This can be an applicable lawful basis for research on personal data that the data subjects themselves have made public or have publicly confirmed, e.g., in an authorized biography, newspaper article or online.

One precondition is that the personal information is published by the person in question, and the data controller (research institution) is responsible for securing and proving / documenting that this is the case[155].

Another condition is that the data subject has intended to make the personal data public. It is the understanding of the task team that information published on Facebook or other internet forums do not necessarily have 'expected publicness' i.e., the information published in these forums is not necessary understood by forum users as 'public' and free to be used for other purposes. This information can therefore not automatically be used in research without further consideration.

In addition, the data controller must ensure that the data subject is capable of understanding the potential positive and negative consequences (immediate and long-term) of making the personal data [156]. One should e.g., not refer to this lawful basis for personal information published by a child, a person suffering from dementia, or others who do not have the cognitive capacity to understand the

[155] Op.cit., GDPR, Art. 24

[156] Op.cit., GDPR, Art. 13 and 5(1) letter a

consequences of publishing. This is considering the GDPR principle of legality and justice set in GDPR article 5 and provisions on consent and on children's special protection when using information services.

For some research projects with internet-based sources, it may be reasonable, after a specific assessment, to assume that the information has been published by the data subject, and that the data subject has consent competence. The GDPR Article 9(2) letter e can then be used as a lawful basis for the treatment, in addition to the basis for treatment in the GDPR Art. 6.

However, the responsibility and burden of proof lies with the data controller, who must be able to document that the conditions in the lawful basis have been met[157]. This can, in many cases, be difficult to secure and prove, making it "safer" for the data controller to refer to the lawful basis in the GDPR Art. 6(1) letter e and Art. 9(2) letter j, as referred to above in section 0 and 0 of this deliverable.

The "disadvantages" of this lawful basis for processing are thus, in the opinion of the task team, that the difficulty of knowing whether the information has been published by the data subject, whether the data subject intended to make the personal data public, and whether the data subject understands the consequences of the publication (is considered competent). Furthermore, it can be difficult for the data controller to document that this is in fact the case.

In addition, the information published by the data subject may contain information about third persons, such as their parents, siblings, friends, and colleagues. This information cannot be processed on the lawful basis of the GDPR Art. 9(2) letter e, because it is not published by the data subject himself/herself. The processing of the information about third persons will therefore need another lawful basis. The GDPR Art. 6(1) letter e and Art. 9(2) letter j, if special categories of personal data are included, will often be an alternative.

A suitable alternative is to obtain consent from the data subjects for the processing of personal data they have published about themselves, or personal data published about them by others. The processing will then have a lawful basis in the GDPR Art. 6(1) letter a, and Art. 9(2) letter a.

5.4 What about the exemptions that allow further processing of personal data for research purposes?

Research projects will often use data sources with personal data originally collected for other purposes. It is not uncommon for personal data collected in one research project to be reused in other research projects.

[157] Op.cit., GDPR, Art. 24

However, the GDPR sets strict requirements for limitations on purpose and storage. These rules apply to all processing of personal data and are guidelines that limit the reuse of data that have previously been collected for other purposes. Still, the law also stipulates exemptions for research. Both the main requirements and the exemptions are stated in the principles presented in GDPR art. 5.

In accordance with the principle of purpose limitation set in GDPR art. 5 letter b, personal data shall be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes»" At the same time, Article 5, presents exemptions made for research purposes, as stating that "further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes".

In accordance with the principle of storage limitation set in GDPR Art. 5(1) letter e, personal data shall be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed". At the same time, exemptions are made for research purposes as GDPR art. 5(1) letter e states that "personal data may be stored for longer periods as far as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation to safeguard the rights and freedoms of the data subject".

The GDPR thus allows for personal data previously collected for other purposes to be further processed for research purposes, and for personal data to be stored for longer than what is normally permitted, as long as the data is only to be used for research purposes. However, there are conditions for the application of these exemptions. A precondition is that appropriate measures are taken to safeguard the rights and freedoms of the data subjects[158]. The GDPR Art. 89(1) specifies that processing "shall be subject to appropriate safeguards, in accordance with the GDPR, for the rights and freedoms of the data subject". The safeguards "shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation". The data controller must therefore take actions not to process more personal data than what is required to fulfil the research purpose. Pseudonymisation is explicitly suggested as a possible measure for data minimisation, provided it does not interfere with the purpose.

Given these exemptions, it is possible to question whether the lawful basis at the start of processing is crucial related to research. Will the exemptions allow for further processing of personal data for research purposes, regardless of the original purpose?

[158] Op.cit., GDPR, Art. 5(1) letter b and e

As mentioned in the introduction of this chapter, the processing of personal data can only take place if the data controller has lawful basis in one of the alternatives of the GDPR Art. 6. In addition, the processing must be covered by one of the exemptions of the GDPR Art. 9, if special categories of personal data shall be processed, and the processing of personal data relating to criminal convictions and offences requires a lawful basis in Member State law (or in Union law). The requirements for lawful basis also apply when research projects use personal data originally collected for other purposes. In other words, further processing is also processing that requires a lawful basis.

The exemptions for research in the principles of purpose limitation and storage limitation may be factors to refer to when documenting the lawful basis for further processing of personal data. This may be particularly relevant when further processing has a lawful basis in the GDPR Art. 6(1) letter e, and possibly art. 9(2) letter j.

However, how to apply the exemptions is not self-evident, seeing as the exemption provisions may be difficult to interpret. It can be challenging for the research institutions to know how the exemptions of Art. 5(1) letters b and e should be understood in practice. It can be questioned to what extent is it legitimate to deviate from the purpose and storage limitation that applied to the original processing, when reusing personal data for research purposes.

If the original processing is based upon consent, the consent given will set conditions for further processing. The data subject may have consented, for example, after being given information that the data will only be used for the original purpose and will be deleted as soon as this purpose is fulfilled. If so, it can be questioned if the exemptions for research in GDPR Art. 5(1), still allow for reuse of the data in research. Such further processing will clearly not be covered by the consent given, and therefore consent, in the task team's opinion, cannot constitute the lawful basis for further processing. However, it can be questioned if further processing for research purposes, beyond what the data subject has consented to, can have lawful basis in the GDPR Art. 6(1) letter e and Art. 9(2) letter j. If so, it can be questioned which measures must be in place to safeguard the rights and freedoms of the data subject[159].

If the original processing has a lawful basis in Art. 6(1) letter e and Art. 9(2) letter j, there will also be conditions related to the processing, i.e., in the form of specific measures and guarantees implemented to safeguard the rights and freedoms of the data subject. For example, the processing may be covered by guarantees against further processing for other purposes and guarantees of deletion. It can then be questioned if the personal data can be freely processed for research purposes, breaching with the original measures/guarantees, if one refers to the exemptions in Art. 5(1) letter b and e, and considers

[159] Op.cit., GDPR, Art. 89(1)

that further processing can take place based on a new lawful basis in GDPR Art. 6(1) letter e and Art. 9(2) letter j.

The two examples above show that it is not necessarily easy to apply the exemptions for research in practice. The law clearly allows for further processing of personal data for research purposes[160]. However, further processing may, in some cases, challenge the principle of fairness and transparency, as well as the overall purpose of the law. If the data subject in connection with the data collection has been given the expectation of purpose limitation and deletion at the end of the original processing, it may be perceived as a violation of privacy if data is processed further – even though the purpose may be in the public interest, e.g., research purposes. In such cases, the data controller must always make a specific assessment of whether the further processing will be lawful, and under which conditions.

It may be challenging for research institutions to argue the lawfulness of further processing when processing is beyond the control of the data subject and contrary to the data subject's reasonable expectations. Legally, there may be uncertainties related to how far the exemptions can legitimately be extended, and what measures should be taken to safeguard the data subjects when further processing personal data for research purposes. Research ethics laws and guidelines may also give reason for caution when further processing personal data in contradiction of consents and necessary guarantees applied to the original processing. Regulatory authorities in European countries may interpret the exemption provisions differently. Research institutions may therefore be concerned about making mistakes, and therefore hesitate in applying the exemptions.

Against this background, it is the task teams understanding that there may be good reasons to look closely at the possibilities of creating a Code of Conduct for the application of the exemptions for research. Such a Code of Conduct could assist the research institutions in operationalizing the GDPR Art. 5(1) letter b and e and provide guidelines for how these can be used when further processing personal data for research purposes.

The lawful basis for the original processing will have an impact on the possibilities for further processing. Therefore, the recommendation of the task team is to start by developing a SSH GDPR Codes of Conduct draft for research that will contribute to obtaining good lawful bases at the time of data collection. Although exemptions may allow for further processing, ensuring a lawful basis when collecting new data is crucial.

[160] Op.cit., GDPR, Art. 5(1) letter b and e

5.5 Why the lawful basis can be an appropriate topic for a Code of Conduct for research

Facilitating long term storage and sharing of research data in Europe is an explicit goal of SSHOC[161]. A prerequisite for achieving this goal is, in the opinion of the task team, to ensure and demonstrate (document) good lawful bases for the processing of personal data used in research. When collecting and reusing personal data, European research institutions must ensure lawful bases for processing that allow for storing and sharing, not only within their own country, but also across national borders within the EU/EEA-area[162]. The processing bases used must be sustainable, to ensure long term and broad access to the data for further use in research.

However, it can be questioned how this can this be achieved when the individual research institution stands alone in interpreting a complicated data protection regulation to find the proper processing basis for the research project.

As shown in section 5.2 of this deliverable, there are both advantages and disadvantages associated with the lawful bases used when processing personal data for research purposes. The most used processing bases all presents challenges regarding the lawfulness of the research. Establishing processing bases that take long term storage and further processing into account, requires both a high competence and careful planning. This applies whether the processing is based upon ‘consent’[163], whether it is “necessary for the performance of a task carried out in the public interest/for scientific research purposes”[164], based on legitimate interests, or it concerns “personal data which are manifestly made public by the data subject”[165]. If research data are collected on a lawful base that is too restricted, implying requirements for deletion or strict conditions for further use, it will be difficult for new research projects to reuse the data. As show above, applying the exemptions from purpose and storage limitation in GDPR Art. 5 may be challenging in practice.

In research, it can be a difficult balancing act to both find a lawful basis that is broad enough to meet the needs for storing and sharing, while also ensuring that the processing safeguards the rights and freedoms of the data subject and does not violate the GDPR. There are good reasons for exploring this issue for research in detail. The individual research institution will benefit from specific guidelines in this

[161] Op.cit., SSHOC project

[162] Op.cit., GDPR Art. 4(2)

[163] Op.cit., GDPR, Art 6(1) letter a and Art. 9(2) letter a

[164] Op.cit., GDPR, Art. 9(2) letter j

[165] Op.cit., GDPR, Art. 6(1) letter f and Art. 9(2) letter e

area, enabling the institution to understand and make use of the possibilities that can be found in the law, while at the same time staying within the framework of the law.

It can, in the task team's opinion, be challenging for the individual research institution to manage such work on its own, because operationalizing the regulations will require both large resources and specialist expertise within several disciplines, including privacy, research and archiving. It can be argued that it will be more appropriate for the specific sector to join forces on this issue. One way to join forces, as the GDPR also encourages, is to establish Code of Conduct[166].

In the view of the task team, it would be a very useful initiative to establish a common SSH GDPR Code of Conduct for research, with purpose on assisting the SSH environment in establishing good bases for processing personal data.

To begin with, the task team will recommend the establishment of Code of Conduct for consent and GDPR art. 6(1) letter a and letter e. It is the task teams' opinion that these lawful bases are commonly used for research purposes and hence suitable for a GDPR SSH Code of Conduct.

As shown in section 5.3.3, the GDPR Art. 6(1) letter f can only be used as lawful basis if the data controller can demonstrate that the controllers' interests are legitimate, and that the rights and freedoms of the data subjects are not overriding these interests. It is the opinion of the task team that it can be safer for research institutions to use GDPR Art. 6(1) letter e as lawful basis for processing of personal data for scientific purposes, pointing out that they are performing a public task, and that they are following the guidelines set in national regulations to give necessary guarantees for the rights and freedoms of the registered.

As shown in section 5.3.4, the GDPR Art. 9(2) letter e can be challenging to use as lawful basis, because it can be difficult for the research institution to ensure and demonstrate that the personal data in question has been published by the data subject, that the data subject intended to make the personal data public, and that data subject understands the consequences of the publication (is considered competent).

As underlined in section 1.2, it is the task team`s understanding that it cannot decide what a SSH GDPR Code of Conduct draft can regulate, as the procedures for developing a Code of Conduct indicates that this must be jointly decided within the SSH Environment.

The scope and issue of the Code of Conduct must be further addressed in Task 8.3.

[166] Op.cit., Report from the European Commission (2020), "Two years of the GDPR: Questions and answers"

5.6 Proposal to create a SSH GDPR Code of Conduct for consent for processing personal data in research

It is the task team's understanding that consent will, in many contexts, constitute a well-functioning lawful basis for processing personal data for research purposes.

One of the great advantages of consent as a lawful basis is that the GDPR in principle provides equal rules for consent in all European countries. The conditions are the same, if the research is carried out in Europe, by European data controllers and / or with European citizens as data subjects. This facilitates that research data based on consent can be processed in Europe under the same conditions. In European research collaborations, this means that, in a somewhat simplified way, that the data controllers do not have to comply with different rules in different countries. This applies if health information, biological and genetic data, and criminal law information are not included in the data material.

Another advantage is that the GDPR allows for relatively broad consents in research, through the exemptions on purpose and storage limitation in art. 5 letter b and e. The task team contemplates that by developing broad consents, one can facilitate long-term storage and sharing of research data across the countries of Europe.

However, it requires both resources and expertise to utilize this space of opportunity for research. For the individual research institution, it can be difficult to be sure how to apply this in research, without coming into conflict with the GDPR. The question is therefore how to develop consents that address the research's need for sharing and long-term storage, without violating the consent requirements of the law?

There are many and, in some cases, strict conditions that must be met for a consent to be valid according to the GDPR. As pointed out in section 0 in this deliverable, this constitutes one of the disadvantages of using consent as a lawful basis. A consent must be informed, voluntary, specific, unambiguous, documentable, and possible to withdraw as easily as it was given[167]. These conditions may be difficult to meet in research.

In some contexts, the consent requirements may be detrimental to the research purpose and / or be practically impossible to fulfil. In such cases, the processing of personal data should then, in the opinion of the task team, have a different lawful basis. In other contexts, however, it may be both beneficial for

[167] Op.cit., GDPR, Art. 40

the research and practically possible to use consent as lawful basis. In both alternatives, consent as a lawful basis can lead to challenges.

In the opinion of the task team, this is because the rules of the GDPR are generally formulated and can be difficult to interpret. For the individual research institution, it may be demanding to understand and operationalize the consent provisions into specific processing of personal data. The application of the regulations requires cutting-edge expertise, especially in research where the GDPR, as mentioned, provides special provisions, e.g., with respect to purpose and storage limitation, which also affects how consent can be formulated.

For data controllers - and perhaps especially for small and medium-sized research institutions - it can be somewhat "unaffordable" to navigate the GDPR, also regarding the provisions on consent. Uncertainty and lack of competence may result in the consent rules not being managed in an appropriate manner in research. This may cause research institutions to carry out research on personal data without securing and proving that the required conditions for consent have been met, or on the contrary, making consents that are "too strict", so that the lawful basis does not cover the necessities of the research.

It is thus no easy task for the individual data controller to formulate consents for their research projects that are both specific enough and that meets other consent requirements in the law, and at the same time are broad enough to cover the necessities of the research. Moreover, this may apply for consent as a lawful basis for long-term storage and further sharing of research data for new research projects. A common European SSH GDPR Code of Conduct for consent in research may remedy some of these problems.

It is the understanding of the task team that the research institutions have a common need for clear guidelines that show how the consent requirements in the GDPR can be operationalized in research. The development of such guidelines will be a demanding task for the individual research institution, as well a poor utilization of resources and competence. A collaboration in the research sector to create guidelines, through a SSH GDPR Code of Conduct, may provide a more cost-effective use of the resources, knowledge and ideas needed.

Through a SSH GDPR Code of Conduct, the research institutions will have access to guidelines that in a simple way demonstrate the requirements for the research to be based on consent, without destroying the purpose of the research. The Code of Conduct will provide guidance in how the conditions of consent can be met in practice the research. It can thus function as support for the individual research institution in the work of ensuring and proving that the consents are legally valid from one project to another.

A SSH GDPR Code of Conduct for consent in research could provide the individual research institution with comprehensible guidelines to comply with, which show how the general privacy rules on consent can be operationalized into a research context. By adhering to such a SSH GDPR Code of Conduct, institutions will be confident that they comply with the regulations when researching personal data based on consent.

A SSH GDPR Code of Conduct for consent in research may also facilitate long-term storage and sharing of personally identifiable research data across national borders in Europe. As mentioned in the introduction of this Chapter, one of the great advantages of consent as a lawful basis is that the conditions are the same throughout Europe. This means that research institutions established in different European countries can join forces to create a template for consent in a specific research project and collect personal data in different European countries based on this consent, and then use the collected personal data for research purposes on equal terms. If the personal data is based on the same consent, the same rules will apply to the further processing of the research data.

By applying the potential of broad consent in research, a SSH GDPR Code of Conduct may show the research institutions how consent should be designed to ensure good utilization and reuse of the research data. The SSH GDPR Code of Conduct can i.e., show how information letters to research participants should be designed, so that the condition of 'informed consent' is met. Furthermore, a SSH GDPR Code of Conduct can provide guidelines on how to ensure that consent is given freely in a research context. This will be beneficial for research that includes vulnerable data subjects.

A SSH GDPR Code of Conduct will also be able to serve as a guide for how research can obtain consents that are unambiguous and explicit enough. This is the main rule set out by the GDPR for consent as a lawful basis. Nevertheless, there is an exception to every rule.

One factor that may complicate a common SSH GDPR Code of Conduct for consent, is that the European countries, pursuant to the GDPR art. 9(4) and art. 10 may provide stricter rules for consent for the processing of health information, genetic and biological, and personal information about criminal convictions and offenses. When preparing a common European SSH GDPR Code of Conduct for consent in research, any differences in national law in these areas must be identified. If differences between the countries are identified, one must consider whether the different rules can be incorporated into the SSH GDPR Code of Conduct, or whether the SSH GDPR Code of Conduct should apply to consent to research that does not include health information, genetic and biological, and personal information about criminal convictions and offenses.

Another factor that may complicate a common European SSH GDPR Code of Conduct for consent is that countries may have different ethical guidelines for consent in research, which partly overlap with, and partly provide additional Codes of Conduct alongside the GDPR. The ethical guidelines may e.g., provide separate definitions or Codes of Conduct for the conditions that must be met for a consent to be given freely, explicit, and informed. The countries in Europe may also have different rules for which ethical approvals are required for the research to be carried out. Hence, variations in research ethics amongst European countries must also be addressed and resolved in the development of a common SSH GDPR Code of Conduct for consent in research.

In summary, it is the understanding of the task team at a creation of an infrastructure concerning consent as lawful basis, the same template for consent can be used by all research institutions in European countries and provide the same conditions for further use of the data.

Consent may constitute a well-functioning lawful basis for the processing of personal data for research purposes. But if a consent is to facilitate the research's need for long-term storage and sharing of data, it presupposes good competence in how the consent should be designed to provide a basis for the desired further use, and a good infrastructure that builds on the consent being given voluntarily, unambiguously, is specific enough, etc. Developing guidelines and templates for broad consensus can be demanding for the individual research institution. It is better for the research sector to work together on this, by developing a SSH GDPR Code of Conduct for consent in research.

One way to facilitate a common European collection of research data with equal conditions for sharing and reuse may be to apply consent as a lawful basis for the processing of personal data. The advantage of consent as a lawful basis is that the conditions are the same throughout Europe, as the GDPR does not allow the countries to make their own rules concerning consent.

Creating a common template for broad consents can be a tool to facilitate the long-term storage, sharing, and reuse of personal data in research European countries. In the process of planning and preparing a SSH GDPR Code of Conduct, this may be a way to go.

5.7 Proposal to create a SSH GDPR Code of Conduct for processing of personal data in the public interest/ for scientific purposes

An advantage of the GDPR art. 6(1) letter e and art. 9(2) letter j as a lawful basis for the processing of personal data for research purposes is that this lawful basis is more flexible than consent. The data controller can largely adapt the privacy measures to the context and the needs of the research, by having more freedom to choose the types of measures that are put in place to protect the data subject's rights and freedoms.

However, this lawful basis may, in the task team's opinion, also present problems for the individual research institution on how to interpret the law. The GDPR art. 6(1) letter e and art. 9(2) letter j have – in accordance with consent – a very general formulation. The lawful basis can often be demanding to understand and operationalize in specific contexts where personal data is to be processed for research purposes. Thus, the institutions can easily make mistakes, either by implementing too strict measures that will create unnecessary obstacles to the purposes, or by invoking a lawful basis without having secured and documented the correct – or many enough – measures for the conditions in the lawful basis to be fulfilled. In addition, in the application of this lawful basis for processing, resources and cutting-edge expertise are required to secure the needs of the researcher, whilst at the same time protecting the data subject. And again, it can be challenging to interpret the special rules that applies for research, which provide exceptions from purpose and storage restrictions (in the GDPR art. 5, letter b and e) if one ensures and demonstrates that the processing is in accordance with art. 89(1).

One of the challenges that institutions may face when using this lawful basis in research, is what information should be given to the data subjects. Information to the data subjects constitutes a key privacy measure that many research projects will be required to implement[168]. As presented in section 5.2 of this deliverable, the GDPR presents many demands on what information should be provided to the data subjects, e.g., in terms of both time, form and content. This apply regardless of the lawful basis for the processing of personal data[169]. It can be difficult for the individual research institution to determine how the information can be designed to provide the research with the necessary conditions, and at the same time arranged for the data subject to exercise his or her rights.

An important measure to facilitate the application of the GDPR art. 6(1) letter e and art. 9(2) letter j as a lawful basis for processing personal information in research may therefore be to design a template for information to the registered. To ensure good conditions for the research environment, in terms of long-term storage and sharing, it is of great importance to affirm how the information to the data subject is designed, whether it is given individually according to art. 13 and 14, or collectively according to art. 14(5) letter b. Information to the data subjects, however, is just one of many possible measures to safeguard the data subject[170].

Another, and just as important, challenge for the research institutions is that it can be difficult to have a complete overview of all measures that can be put in place in order to protect the data subject's rights and freedoms. To remedy this, the task team considers that it would be appropriate for the research sector in Europe to work together to create an overview of all privacy measures that can be implemented as necessary guarantees. Such an overview can be included in a Code of Conduct for research based on the GDPR art. 6(1) letter e and art. 9(2) letter j.

A third challenge, which the relevant lawful basis shares with consent, is that the research institutions must comply with research ethics guidelines that partly overlap with, and partly supplement, the GDPR. The ethical guidelines, including the rules for ethical approvals, may vary between countries in Europe, and thus present different guidelines for research on personal data that have a lawful basis in the GDPR art. 6(1) letter e and art. 9(2) letter j.

The main disadvantage of the lawful basis is, as presented in section 0 of this Deliverable, the requirement of a supplementary lawful basis[171]. The GDPR allows for different laws in different European countries, which can provide different conditions for research on personal data that is not based on consent. The lawful conditions for personal data that are processed on this lawful basis can, in the task

[168] Op.cit., GDPR, Art. 13
[169] Ibidem
[170] Op.cit., GDPR, Recital 108 Appropriate Safeguards
[171] Op.cit., GDPR, Art. 6(1) letter e and art. 9(2) letter j

team's opinion, thus vary - to some extent strongly - amongst the countries in the EU / EEA. This makes it challenging to use the GDPR art. 6(1) letter e and art. 9(2) letter j as a lawful basis, especially in research where it is preferable to facilitate the sharing and reuse of data across countries in Europe. Moreover, this presents a big paradox. The lawful basis that was designed to facilitate research on personal data thus in part places major obstacles for European research collaboration, and for further processing of research data across national borders, through the requirement for a supplementary lawful basis.

A SSH GDPR Code of Conduct that attempts to operationalise this lawful basis for research can, and must, address these issues. One must also dare to ask the honest question whether the supplementary lawful bases in themselves can make it difficult to develop a SSH GDPR Code of Conduct with this topic. One measure to remedy the situation may, however, be to let the mentioned overview of privacy measures specify in which countries the various measures are defined as mandatory, by mapping the national supplementary lawful bases. Such an overview can help institutions from different countries that plan research collaboration to consider - and implement - all the measures that are mandatory in the relevant countries included in the research, as part of providing a lawful basis for the processing in the GDPR art. 6(1) letter e and art. 9(2) letter j.

Another potentially great advantage of such an overview is that it can make it clear to European authorities that one of the purposes of the GDPR, namely, to simplify and harmonise the rules for research and facilitate transnational research collaboration in Europe, is far from being achieved. It may emphasize the need for common rules for the operationalization of this lawful basis, which are specifically intended for research. An important argument is that the supplementary lawful basis cannot only be established in the member states' national law, but also in Union law[172]. It is thus possible for the EU to create common rules for how research can meet the conditions in the GDPR art. 6(1) letter e and art. 9(2) letter j. A SSH GDPR Code of Conduct for this lawful basis in research - or the attempt to create one - may demonstrate the need for the Union to formulate such common rules.

In summary, the GDPR art. 6(1) letter e and art. 9(2) letter j provide more flexible conditions for research than consent. However, for the individual research institution, it is often an art of balance to find the right type and number of measures to safeguard the data subjects, without hindering the research. This is especially true when for a lawful basis that allows for long-term storage, further sharing, and reuse of the research data for new research projects. It is therefore important to explore the possibilities for creating a SSH GDPR Code of Conduct for research based on this lawful basis. Due to the requirement for a supplementary lawful basis, it can be challenging to create a common European Code of Conduct for this lawful basis. The task team believes that it will be useful to try, i.e., by identifying which privacy

[172] Ibidem

measures can be implemented, and which measures are required in the different European countries to meet the conditions of the lawful basis.

6. Stakeholder analysis

As mentioned in section 3 of this deliverable, when creating a SSH GDPR Code of Conduct draft relevant stakeholders, including data subjects, should be consulted, confirming, and demonstrating that an appropriate level of consultation has been performed[173].

According to guidelines presented by EDPB, the draft can include "...information about other codes of conducts that potential code members may be subject to and reflect how their code complements other codes. This should also outline the level and nature of consultation which took place with their members, other stakeholders and data subjects or associations/bodies representing them"[174].

For the further work on initiating a SSH GDPR Code of Conduct, relevant stakeholders should therefore be identified. The task team has in this Deliverable started the work on performing a Stakeholder analysis. This analyse is presented in the following Table. Note that this must be further developed, and a plan for how this should be actioned can be made in the further work in WP8.

TABLE 1 STAKEHOLDERS: STAKEHOLDERS' INFLUENCE AND CONTRIBUTION TO THE CODE OF CONDUCT

Stakeholders	How will they influence the work and what can they contribute to	Will they be affected by a Code of Conduct and how?
Researchers	Can help determine the scope of the SSH GDPR Code of Conduct. Inform if subject to other Code of Conducts, enabling the understanding on how a SSH GDPR Code of Conduct complements possible other codes.	Depending on the scope of the SSH GDPR Code of Conduct. Will be able to share and reuse data. Will have one set of guidelines to use.

[173] Op.cit., GDPR, Recital 99

[174] Op.cit., EDPB's Guidelines, section 28

Research institutions	Can help determine the scope of the SSH GDPR Code of Conduct Inform if subject to other Code of Conducts, enabling the understanding on how a SSH GDPR Code of Conduct complements possible other codes.	Its obligations and responsibilities as data controller or processor under the GDPR will be fulfilled.
Data subjects (participants in research projects)	Can help determine the scope of the SSH GDPR Code of Conduct	Its freedoms and rights will be protected and managed at the same way within the European SSH Environment.
Supervisory authorities	Can provide information on necessary steps to be able to create a SSH GDPR Code of Conduct draft and how to get it approved. Can also assist in the assessment on how the terms in GDPR art 40 and 41 are to be interpreted. The competent supervisory authority must assess the draft and if admissible, take it to the next level to get it approved.	Will be able to provide guidance to the SSH Environment about the existence of a Code of Conduct, and to understand the conditions and needs that arises within the SSH environment, compared to other areas of society.
European data protection Board (EDPB)	Can provide information on necessary steps to be able to create a SSH GDPR Code of Conduct draft and how to get it approved. Can also assist in the assessment on how the terms in GDPR art 40 and 41 are to be interpreted. Must approve the SSH GDPR Code of Conduct.	Will be able to provide guidance to the SSH Environment about the existence of a Code of Conduct, and to understand the conditions and needs that arises within the SSH environment, compared to other areas of society.
Data archives	Can help determine the scope of the SSH GDPR Code of Conduct	Depending on the scope of the SSH GDPR Code of Conduct. Will be able to share data easier, due the facilitation and

	Inform if subject to other Code of Conducts, enabling the understanding on how a SSH GDPR Code of Conduct complements possible other codes.	transparency for data subjects and planned lifecycle of personal data.
EOSC	Can help determine the scope of the SSH GDPR Code of Conduct Inform if subject to other Code of Conducts, enabling the understanding on how a SSH GDPR Code of Conduct complements possible other codes.	Depending on the scope of the SSH GDPR Code of Conduct. Will be able to share data easier, due the facilitation and transparency for data subjects and planned lifecycle of personal data.
CESSDA	To facilitate the creation of a SSH GDPR Code of Conduct	
NSD	To facilitate the creation of a SSH GDPR Code of Conduct	
BBMRI ERIC and other institutions with experiences crating Code of Conducts	To facilitate the creation of a SSH GDPR Code of Conduct, by providing information on their experiences working on a Code of Conduct. Assess if a SSH GDPR Code of Conduct complements their work on a Code of Conduct.	Can benefit considering shared experiences and facilitation.
The responsible parties for financing the creation and monitoring of a SSH GDPR Code of Conduct	To facilitate the creation of a SSH GDPR Code of Conduct, determining resources and timeframe.	
Other authorities, such as Ministry of Education	Can help determine the scope of the SSH GDPR Code of Conduct	
Interest groups for participants	Providing input on freedoms and rights, making sure data subjects will	Their member`s freedoms and rights will be protected and

	be protected.	managed at the same way within the European SSH Environment.
Register managers	Can help determine the scope of the SSH GDPR Code of Conduct Inform if subject to other Code of Conducts, enabling the understanding on how a SSH GDPR Code of Conduct complements possible other codes.	
EU commission	Must approve the SSH GDPR Code of Conduct.	Aiming its statement as the creation and use of a SSH GDPR Codes of Conduct can be an important tool to ensure harmonisation.

7. Conclusions and next steps

The initiative laid down in this Deliverable, represents a starting point of the initiate to create a SSH GDPR Code of Conduct. It will be necessary with a significant collaboration between stakeholders within the SSH environment to enable a SSH GDPR Code of Conduct draft to be written and submitted. However, the creation of a SSH Code of Conduct can, in the opinion of the task team, be of great benefit for the SSH Environment and the environment should be encouraged to collaborate in further work.

Going further, it is recommended that a plan should be made on how to fulfil the procedural terms presented in Chapter 4 of this Deliverable. It will also be necessary to determine what a SSH GDPR Code of Conduct should regulate, derby determining the scope of it. It will also be important to determine which body should be responsible for drafting.

It is further recommended that work includes an assessment of which scope and purpose a SSH GDPR Code of Conduct should regulate, derby determining the need within the specific sector. It must, for instance, be determined if it will apply for parts of the SSH Environment, or if it shall apply in general. This is also likely to affect what it should regulate, as it should be able to represent issues in that concrete sector and processing activities.

In section 5 of this deliverable, some suggestions of content have been presented. However, the aim of this task doesn't encompass the scope of SSH GDPR Code of Conduct regulation, as the procedures for developing a Code of Conduct indicates that this must be jointly decided within the SSH Environment[175]. Therefore, different stakeholders within the SSH Environment should be consulted on the area of regulation, determining the scope of the Code. This deliverable also initiated the work on a Stakeholder analysis, presented in section 6. This analysis should be further developed, including addressing which persons/bodies are of interest and how they can be included in the initiative to create a SSH GDPR Code of Conduct.

The upcoming work in Task 8.3 in WP8 should also determine if the SSH GDPR Code of Conduct will be defined as an international Code, assess which bodies are able to represent the SSH Environment, and which supervisory authorities can be considered competent. It is also recommended that the upcoming work includes an assessment of monitoring mechanisms. As the content of a SSH GDPR Code of Conduct must be compliant with national legislation, relevant national legislation should be identified. SSH GDPR Code of Conduct is likely to be international, therefore a plan should be made on how this will be managed for all involved countries.

[175] Op.cit., EDPB's Guidelines, chapter 5

References

The European Data Protection Board: EDPB

EDPB`s guidelines and appendices used:

1. EPDB`s guidelines Chapter 1
2. EDPB`s guidelines Section 3
3. EDPB`s guidelines Chapter 3 - 6
4. EDPB`s guidelines section 12
5. EDPB`s guidelines Section 19 - 27
6. EDPB`s guidelines section 29 - 30
7. EDPB`s Appendix 2

The GDRP Articles

1. GDPR art. 1
2. GDPR art. 4 – 10
3. GDPR art. 12 - 14
4. GDPR art. 22
5. GDPR art. 24 - 26
6. GDPR art. 28 - 29
7. GDPR art. 32
8. GDPR art. 34 - 37
9. GDPR art. 39 - 41
10. GDPR art. 51
11. GDPR art. 55
12. GDPR art. 89

The GDPR Chapters and Recitals

1. GDPR Chapter 1 of the GDPR
2. GDPR Chapter 5 of the GDPR
3. GDPR Recital 42 - 43 of the GDPR
4. GDPR Recital 99 of the GDPR
5. GDPR Recital 108 of the GDPR
6. GDPR Recital 122 of the GDPR

Other references:

Article 29 Data Protection Working Party; Opinion 15/2011
https://ec.europa.eu/justice/article-29/documentation/opinion
recommendation/files/2011/wp187_en.pdf

DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&rid=5

Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679
https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-0_en

The General Data Protection Act
https://gdpr-info.eu/

GDPR, Consent requirements
https://gdpr.eu/gdpr-consent-requirements/

IOC Legitimate interests
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/

Social Sciences & Humanities Open Cloud (SSHOC)

a. Social Sciences & Humanities Open Cloud (SSHOC)
   https://www.cessda.eu/About/Projects/Current-projects/SSHOC
b. SSHOC workshop
   https://zenodo.org/record/4655623#.YNrBnukzZp8

What is GDPR, the EU's new data protection law?
https://gdpr.eu/what-is-gdpr/