Research and Innovation Action

Social Sciences & Humanities Open Cloud

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

Deliverable 8.5 Recommendations for a GDPR Code of Conduct for SSH

Dissemination Level	PU
Due Date of Deliverable	30/04/2022 (M40)
Actual Submission Date	29/04/2022
Work Package	WP 8 - Governance/ Sustainability/ Quality Assurance
Task	Task 8.3 Legal and Ethical Issues
Type	Report
Approval Status	Waiting for EC approval
Version	V1.0
Number of Pages	p.1 – p. 39

Abstract:

This report intends to initiate a draft SSH GDPR Code of Conduct to be created. It describes necessary actions to create one and provides recommendations on how these terms can be fulfilled. Some suggestions on what an SSH GDPR Code of Conduct can regulate is also included.

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
0.1	26/10/2021	First draft	Authors
0.2	27/10/2021	Review	Siri Tenden (Sikt)
0.3	15/11/2021	First draft ready for peer review	Authors
0.4	23/11/2021	Peer review done	Emiliano Degl'Innocenti (CNR), Maurizio Sanesi (CNR)
0.5	25/11/2021	Second draft ready for WP-leaders review	Authors
0.6	07/12/2021	Third draft including additional input, ready for WP-leaders review	Authors
0.7	09/12/2021	Coordinator review	Martina Drascic Capar (CESSDA ERIC), Ivana Ilijasic Versic (CESSDA ERIC)
0.8	13/12/2021	Fourth draft	Authors
0.9	14/12/2021	3rd peer-review	Eva J. B. Payne (Sikt), Christopher Autzen (Sikt)
0.10	15/12/2021	Fifth draft send to CO	Authors
0.11	03/03/2022	4th peer-review done (1st Tier)	Silvana Muscella, (Trust-IT), Astrid Verheusen (LIBER), Jennifer Edmond (DARIAH), Pawel Kamocki, the chair of the CLARIN Legal and Ethical Issues Committee (CLIC)
0.12	01/04/2022	Sixth draft after peer-review	Authors
1.0	28/04/2022	Final version ready for submission to the EC	CESSDA ERIC

Author List

Organisation	Name	Contact Information
CESSDA ERIC/Sikt	Ina Nepstad	Ina.nepstad@sikt.no
CESSDA ERIC/Sikt	Mathilde Steinsvåg Hansen	Mathilde.hansen@sikt.no
CESSDA ERIC/Sikt	Inga Brautaset	Inga.brautaset@sikt.no
CESSDA ERIC/Sikt	Lisa Lie Bjordal	Lisa.bjordal@sikt.no
CESSDA ERIC/Sikt	Njaal Hendrik Neckelmann	Njaal.Neckelmann@sikt.no
CESSDA ERIC/Sikt	Marianne Høgetveit Myhren	Marianne.Myhren@sikt.no
CESSDA ERIC/NSD	Ingvild Eide Graff	Ingvild.Graff@nsd.no
CESSDA ERIC/Sikt	Vigdis Namtvedt Kvalheim	Vigdis.Kvalheim@sikt.no

Executive Summary

Background: The General Data Protection Regulation (EU) 2016/679 (hereinafter GDPR) has given EU/EEA countries an opportunity to harmonise their legal framework for data protection, and to improve the conditions for processing personal data in research and data sharing. Although this was one of the rationales behind the GDPR, it has not necessarily been achieved [1-3].

Main aim: To facilitate harmonisation across the EU/EEA and sectors, the European Union Commission (hereinafter EC) has highlighted the creation and use of Codes of Conduct [4]. A Social Science and Humanities (hereinafter SSH) GDPR Code of Conduct may lead to such a harmonised practice within the SSH environment [1]. This report intends to give a set of recommendations for how an SSH GDPR Code of Conduct can be created [1].

Methodology: This report is developed as a result of the input from SSHOC WP5, Innovations in Data Access (T5.3 Legal Issues of innovative data access). The report "Draft SSH GDPR Code of Conduct" started the initiative of creating an SSH GDPR Code of Conduct draft. This report intends to further this initiative. This is done by elaborating on the conditions that must be met in order to have a Code of Conduct approved, which are set up in The GDPR Article 40 and 41 [5, 6]. Some of these conditions may be particularly important to address early in the process when initiating a Code of Conduct. In addition, partners/stakeholders have been consulted.

Main outcome: The creation of an SSH GDPR Code of Conduct requires several terms to be fulfilled, before it will be approved. Building on the report "Draft SSH GDPR Code of Conduct", this report describes these terms, suggests how they can be fulfilled and presents input from consulted partners. In sum, the report identifies the following terms that must be fulfilled in order to make a Code of Conduct draft admissible: it must be determined which organization(s) have the mandate to draft the Code; specific explanatory statements and supporting documents must be gathered, the territorial and processing scope of the Code must be determined. Further, it must be determined which supervisory authority is competent to assess and approve the Code draft; which monitoring body is appropriate for the Code and which mechanisms will enable that monitoring body to perform its task. In addition, consultation with stakeholders must be performed; and the draft Code must be in compliance with relevant national legislation and the content and language of the Code must be determined. This report presents recommendations on how the initial steps/terms can be fulfilled to get an SSH GDPR Code of Conduct draft created and admissible.

The report presents a suggested framework for the initial steps of consulting the sector to identify and document its needs, to find and agree on an organization or body that can represent the SSH Environment and to determine the potential processing and territorial scope of the SSH GDPR Code of Conduct. The initiative is a first step in specifying what remains of further work. These factors may facilitate the continuation of the work of realizing an SSH GDPR Code of Conduct, which will be of great benefit to EOSC, the research environment, data sharing and society at large.

Conclusion: A draft Code must document that relevant stakeholders have been adequately consulted on the need for a draft Code, its scope and its content. The report contains input from partners and one supervisory authority. Many of the elements that need to be decided on further along in the process are contingent upon elements on which the SSH research environment must voice their opinions. In order to effectively progress with the work on a draft Code, it will be essential that the stakeholders are involved. This report furthers the suggestions addressed in the report "Draft SSH GDPR Code of Conduct" on what an SSH GDPR Code of Conduct can regulate [1].

Abbreviations and Acronyms

BBMRI ERIC	European research infrastructure consortium (ERIC) for biobanking; https://www.bbmri-eric.eu/about/
CESSDA ERIC	Consortium of European Social Science Data Archives
CLIC	Clarin Legal and Ethical committee
CNIL	Commission nationale de l'informatique et des libertés; French supervisory authorities
CNR	Consiglio Nazionale delle Ricerche
Controller	The 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.
CLARIN ERIC	Common Language Resources and Technology Infrastructure
CLARIN ERIC CLIC	Common Language Resources and Technology Infrastructure, Legal and Ethical Issues Committee
DARIAH ERIC	Consortium of Digital Research Infrastructure for the Arts and Humanities
EASSH	European alliance for social sciences and humanities
EC	The European Commission
EDPB	European Data Protection Board
EEA	European Economic Area
ELDAH	Ethics and Legality in the Digital Arts and Humanities
EOSC	European Open Science Cloud
ESS ERIC	European Social Survey European Research Infrastructure
EU	European Union

EUCROF	European CRO Federation
GDPR	The General Data Protection Regulation (EU) 2016/679
LERU	League of European research universities
NSD	NSD - Norwegian centre for research data
Processor	A 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 is regulated by an agreement.
RDM	Research data management
SHARE ERIC	Consortium of survey of Health, Ageing and Retirement in Europe
Sikt	Sikt - Norwegian Agency for Shared Services in Education and Research
SSH	Social Science and Humanities
SSHOC	The Horizon 2020 project “Social Science & Humanities Open Cloud”
WP	Work package

Table of contents

1 Introduction

This report provides a set of recommendations for the process of establishing a common GDPR Code of Conduct for SSH. The overall aim is to contribute to a legal and ethical framework for SSH research that handles uncertainties and contribute to consistent and sustainable data-sharing rules and practices across countries, legal systems, and cultures to support the realisation of the EOSC.

Research data collected, used, and reused by the SSH community often contains personal data. Hence, and in accordance with the GDPR art. 24, each institution is required to ensure and demonstrate that they comply with the GDPR. The GDPR encourages the use of approved Codes of Conduct as a tool to ensure correct legal application and demonstrate compliance with the GDPR [5]. The GDPR has given Europe an opportunity to harmonise the legal framework for data protection and to improve the conditions for processing personal data in research and cross-border data sharing [1, 2] the various research domains, data producing institutions, data archives and other infrastructures within the SSH environment with the opportunity to develop GDPR compliant Code of Conducts in order to facilitate a harmonised legal practice regarding data access and data sharing.

Experience within and across European countries demonstrate that it can be difficult to interpret the general rules in the GDPR and to understand how they apply to the various fields of research. Different interpretations of the regulation can result in different terms of use of personal data for research purposes, which in turn can make it difficult to store and share data across national borders in Europe.

1.1 What is a Code of Conduct in the GDPR?

The GDPR is a general law, meaning that it applies to all activities, not only research. A Code of Conduct can, in accordance with GDPR, be made, as a supplement to the GDPR to provide guidance on how to act within the Regulation in specific areas. Unlike informal codes of conduct, a Code of Conduct based on Article 40 of the GDPR is formalized through several conditions that must be met before it can be approved by the supervisory authorities. Thus, to establish a Code of Conduct and to get it approved is a comprehensive process.

According to the EDPB Guidelines 1/2019 on Codes of Conduct, A Code of Conduct is a set of rules for a specific sector that provides guidelines on how the companies in that sector must adapt to comply with the requirements in the GDPR [7] . A Code can be understood as a mean to "translate" the general rules of the GDPR into more sector-specific guidelines, assisting the institutions with practical tools that enable them to perform their activities in accordance with the law. The EDPB points out that from a data protection viewpoint, codes can therefore operate as a rulebook for institutions to design and implement GDPR compliant data processing activities which give operational meaning to the principles of data protection set out in European and National law. A GDPR Code of Conduct is developed by the sector itself, before it is eventually approved by the Supervisory Authority [8, 9].

1.2 Benefits of an SSH GDPR Code of Conduct

For the SSH sector, it may at first glance seem unnecessary to invest a lot of work in creating and agreeing on formal guidelines, in terms of an SSH GDPR Code of Conduct. After all, the sector has already established various templates and best practices that seems to work relatively well. However, it can be argued that the formalization of guidelines, through an approved Code of Conduct, has many advantages.

Using standards for the processing of personal data can make it easier to allow research data to shared and be used over time and across countries within Europe. This will in turn facilitate cross-border research cooperation and long-term reuse of research data collected in different European countries.

An SSH GDPR Code of Conduct can improve conditions for research and support the realisation of the EOSC, by harmonising the legal framework for data processing across Europe and facilitating long-term data storage and cross-border data flow [1]. The report "Draft SSH GDPR Code of Conduct", Chapter 2, provides further explanations on what a Code of Conduct is and what the purpose and benefit will be for the SSH Environment [1]. In sum, and as emphasised in the report, a Code of Conduct can make it easier for the SSH Environment to operate in accordance with the GDPR and at the same time facilitate data access and use. It may also reduce administrative burden of demonstrating compliance with the Regulation, and reduce risks of sanctions and correlating reputational loss, as acting in accordance with the Code will be within the rules set in the Regulation, approved by a Supervisory Authority.

To facilitate harmonisation across EU/EEA and sectors, and the realisation of EOSC, the EC has also highlighted the creation and use of Codes of Conduct as an important tool [4]. An SSH GDPR Code of Conduct may lead to such a harmonised practice within the SSH community [1]. This could give the SSH environment an opportunity to create a formal common framework to demonstrate compliance and facilitate harmonisation of data-sharing rules and practices [2].

1.3 Scope of report

This report builds on valuable input from WP5, Innovations in Data Access (T5.3 Legal Issues of innovative data access), which recommended exploring the possibility of developing a common Code of Conduct [10]. T5.3 delivered the report "Draft SSH GDPR Code of Conduct", which started the initiative of creating an SSH GDPR Code of Conduct draft [1]. The report briefly discussed the terms set out in GDPR art. 40, and suggested what an SSH GDPR Code of Conduct may regulate, leaning among others on results from SSHOC Deliverable 5.7 and 5.19 and the BBMRI-ERIC`s work on a health and life Science GDPR Code of Conduct [2, 3].

This report builds on this initiative by suggesting a framework for how the initiative should be expanded on in further work and by giving a set of recommendations on the process of establishing a draft Code of Conduct that can be approved by a supervisory authority.

The work has been based on interpretations of the GDPR, published reports, documents and guidelines. The report also suggests what an SSH GDPR Code of Conduct can regulate.

Being able to plan and perform the work to get a draft Code of Conduct admissible, presupposes detailed knowledge of the legal requirements set in GDPR, as well as the regulating the process. Chapter 2 of this report therefore investigates in more detail what the procedural conditions in GDPR art. 40 implies in SSH context. To fulfil these terms for an SSH GDPR Code of Conduct, the report presents a suggested framework that in further work can be used for the initial steps of consulting the sector to identify and document its needs, to find and agree on an organization or body that can represent the SSH Environment and to determine the potential processing and territorial scope of the SSH GDPR Code of Conduct. This is a first step which specify what remains in further work, aiming to facilitate the continuation of the work of realizing an SSH GDPR Code of Conduct. An SSH GDPR Code of Conduct for the SSH could undoubtedly be of great benefit to EOSC, the research environment, data sharing and society at large.

The report "Draft SSH GDPR Code of Conduct" recommended that stakeholders should be consulted on procedural terms to get a Code of Conduct approved. Task partners (SHARE ERIC, CLARIN ERIC, DARIAH ERIC, ESS ERIC and CNR and CESSDA ERIC), who are representatives from the SSH research community throughout the EU/EEA, and at the same time important stakeholders, have provided input on how these terms can be interpreted and actioned. They all have valuable insights into European social sciences and humanities as a whole and processing of personal data by this sector.

The partners were asked ten questions on how, in their opinion, the initiative should be furthered and what an SSH GDPR Code of Conduct should regulate. The questions were created based on the terms set in the GDPR Articles 40 and 41 on how to get an SSH GDPR Code of Conduct draft approved.

The establishment of a GDPR Code of Conduct has its legal basis in GDPR article 40 and 41 [5, 6]. The development of such a Code must thus adhere to the requirements set out in these GDPR articles. The articles and terms are complex, and it can be difficult to understand how to fulfil them in practice. Within each EU/EEA country, a supervisory authority has, among other things, been assigned the task of providing guidance on how to comply with the GDPR. Further, supervisory authorities are to approve Codes of Conduct and encourage the creation of Codes of Conduct [8, 9, 11]. Therefore, the Norwegian supervisory authority, Datatilsynet, was asked whether the terms in GDPR Article 40 were correctly interpreted and to provide more guidance on how to interpret them.

As the GDPR regulations on Codes of Conduct applies to all EU/EEA countries and each supervisory authority must assess a Code of Conduct based on the same terms, the response from the Norwegian supervisory authority is applicable in all EU/EEA countries. A response from one supervisory authority can therefore be generalised to EU/EEA countries in general and will therefore be of relevance for a cross-border Code of Conduct.

The report "Draft SSH GDPR Code of Conduct" suggested what an SSH GDPR Code of Conduct might regulate, which is presented and supported in Chapter 3 of this report. Note that these initiatives combined do not [1,

7] have the mandate to decide what an SSH GDPR Code of Conduct draft shall regulate, as the procedures for developing a Code of Conduct indicates that this must be jointly decided within the SSH Environment [2, 7].

1.4 The importance of contributions from stakeholders

An underlying premise for the whole concept of Codes of Conduct is that the Codes must be firmly anchored within the sector that is indeed supposed to own and use it. Consultations with relevant stakeholders are particularly important to ensure that the Code is designed in line with the needs of the sector, so that it becomes useful. In addition, such consultations are essential to gain support and trust from the sector and will increase the chances that the Code will be implemented and adhered to. These aspects probably constitute some of the rationale behind the legal requirement to document consultation with stakeholders before a draft Code of Conduct can be approved.

The GDPR Article 40 and 41 set up several conditions that must be met to create an SSH GDPR Code of Conduct [1, 5, 6]. Some of these conditions can be particularly important to address early in the process. For instance, it is crucial to find a representative of the SSH Environment that can lead the work of drafting the Code. Moreover, it is pivotal to examine the needs of the sector properly, to determine how the material and territorial scope of the Code should be defined. Thus, the SSH Environment must investigate and decide how the Code should be designed for it to benefit European research. The basis for deciding its scope, and the fact that the draft upholds requirements set out in the GDPR, must be adequately documented [1, 5-7].

The initial steps of developing an SSH GDPR Code of Conduct cannot be done by a small group alone, and it is necessary that this work has a solid foundation in the SSH Environment from the very beginning [1]. As part of the initiative to establish an SSH GDPR Code of Conduct, the report “Draft SSH GDPR Code of Conduct” stressed the importance of consulting relevant stakeholders [1]. Therefore, partners have been asked to provide valuable contributions. In addition, a Data Protection Authority has also been consulted. As a supervisory authority, they have considerable insight and may provide useful guidance concerning the preparation of a draft Code [8, 9].

2 Procedural steps to get an SSH GDPR Code of Conduct admissible

The GDPR Articles 40 and 41 provides information on what an SSH GDPR Code of Conduct can regulate, and which procedural steps are necessary for the approval of an SSH GDPR Code of Conduct [5].

The report "Draft SSH GDPR Code of Conduct" identified briefly which terms must be fulfilled to make a draft Code of Conduct admissible [1]. In the following, a further elaboration of what these terms entail is presented.

The content of the terms is identified through an interpretation of the GDPR Articles 40 and 41 and by studying the guidelines on Codes of Conduct and monitoring bodies published by the EDPB [5-7]. The guidelines are meant to explain how GDPR Articles 40 and 41 are to be practised [7].

As the following shows, multiple procedural actions must be taken before a draft SSH GDPR Code of Conduct can be evaluated and considered admissible. The terms are set to enable an effective evaluation of any draft Code [10] and will therefore be relevant for further work.

2.1 Who should represent the SSH Environment?

The EDPB Guidelines have included a non-exhaustive list of possible Code owners [7]. This list specifically includes trade and representative associations, sectoral organizations, academic organizations and interest groups [7]. The EDPB Guidelines further reference the Article 29 Working Party document concerning industry self-regulation and recommend that this document should be considered, where relevant, when formulating a Code of conduct [7].

The referenced document, WP7 adopted January 14th, 1998, states that an "important criterion for judging the value of a Code is the degree to which its rules can be enforced". The document elaborates this in a segment on how the value of the Code will be strengthened if the Code and responsible body (under the current GDPR, "Code owner") coverage is industry- or profession wide. From a consumer standpoint, a fragmented industry with rival associations and potentially competing data protection Codes will be confusing and would likely cause a lack of transparency. It could also impede the ability to effectively impose sanctions on Code members [12].

In the context of an SSH GDPR Code of Conduct, corresponding arguments concerning transparency could be made for both data subjects and researchers, institutions and organizations aiming to contribute or access data for research or research archiving purposes. Ensuring that a Code owner can represent an entire category of data controllers and processors, is related to the overall aim of GDPR Codes of Conduct and contributes to the effective application of the GDPR. Finding a suitable representative Code owner will also contribute to the effective realization of the aims of EOSC and SSHOC. The ability to represent a category of data controllers and processors is also related to the specific

approval requirements concerning effective mechanisms and structures that ensure that an SSH GDPR Code of Conduct can be effectively enforced.

2.2 Explanatory statement and supporting documents

An SSH GDPR Code of Conduct draft must contain specific explanatory statements that explain and justify the scope and purpose of the Code [1, 7]. The draft must also explain how the Code will facilitate the effective application of the GDPR. In addition, the draft must be supported by documents that demonstrate the need for an SSH GDPR Code of Conduct [1, 7]. For instance, the Code draft could include documentation from interviews, workshops and/or surveys within the SSH environment [1].

The EDPB Guidelines provide more substantive guidance concerning the draft Code, explanatory statement and supporting documentation. According to the guidelines, the explanatory statement must be clear and concise. Amongst other things, the explanatory statement will assist in expediting the process and providing the requisite clarity to accompany a submission [7].

The explanatory statement must provide details as to the purpose of the Code. It must demonstrate how the proposed Code meets a particular need of that sector or processing activity. The Code owners "should be able to explain and set out the problems the Code seeks to address and substantiate how the solutions the Code offers will be effective and beneficial not only for their members but also for data subjects" [7]. Furthermore, it must clearly define the scope in which it applies, both in terms of processing activities, and in terms of its territorial scope [7].

The explanatory statement must demonstrate how it will contribute to the proper application of the GDPR – both in facilitating and in specifying how the GDPR should be applied within the sector [7]. In doing so, it must take account of the specific features of the processing sector, and the specific requirements and obligations of the controllers or processors to whom the Code relates [10]. The standards must be realistic and attainable for all the Code members, and "need to be of a necessary quality and internal consistency to provide sufficient added value" [7]. The draft Code "will need to be adequately focused on particular data protection areas and issues in the specific sector to which it applies, and it will need to provide sufficiently clear and effective solutions to address those areas and issues" [7].

The explanatory statement must also demonstrate that the Code will provide sufficient safeguards. These safeguards must be adapted according to the risk and sensitivity of the data processing to which they apply. The guidelines exemplify this by noting that "'high risk' sectors, such as processing children's or health data would be expected to contain more robust and stringent safeguards, given the sensitivity of the personal data in question" [7]. In addition, the explanatory statement must demonstrate that the Code will provide effective mechanisms for monitoring compliance with a Code [7].

Where relevant, the submission of the draft Code must include supporting documentation to underpin the draft Code and explanatory statement [7].

The checklist provided by the EDPB, in Appendix 3 of the guidelines, arguably constitutes a useful summary of the elements in a draft Code that require documentation:

- That the submitting association or other body represents categories of controllers or processors
- Details to substantiate that the aforementioned association or body is an effective representative body capable of understanding the needs of its members
- The processing activity or sector and the processing problems the Code intends to address is clearly defined
- Identification of the territorial scope of the Code; inclusion of a list of all concerned Supervisory Authorities
- Details to justify the identification of the competent supervisory authority
- How the Code provides mechanisms that allow for effective monitoring of compliance
- Identification of a monitoring body, and an explanation as to how it will fulfil the Code monitoring requirements
- Information as to the extent of consultation carried out in developing the Code
- Confirmation that the draft Code is compliant with Member State law(s) (where relevant)
- That the language requirements are met
- Sufficient details to demonstrate the proper application of the GDPR

2.3 Processing and territorial scope

To make a draft SSH GDPR Code of Conduct admissible, it will be necessary to give a precise description of the Code´s processing and territorial scope [7]. This means that the Code draft must explain clearly which categories of data controllers and processors the Code will govern, and which processing operations of personal data it applies to. A draft SSH GDPR Code of Conduct must also describe which country/countries the Code will cover [1].

2.4 Supervisory authority

An SSH GDPR Code of Conduct draft must be submitted to and assessed by a competent supervisory authority [1]. All EU/EEA countries must provide an independent public authority responsible for monitoring the application of the GDPR. The Code owners are responsible for identifying which competent supervisory authority should assess the Code draft [1].

For Codes of conduct with a national territorial scope, this decision is straightforward. If one wishes to pursue an SHH GDPR Code of Conduct with a transnational territorial scope, however, the Code owners must assess which competent supervisory authority is deemed most appropriate. The EDPB Guidelines has a non-exhaustive list of factors that can be considered in this assessment:

- 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 [7]

The process of assessing the draft Code will from the point of submission be coordinated by the supervisory authority, seeking advice and opinions from other relevant supervisory authorities, as outlined in the EDPB Guidelines chapter 8.3 [7].

The EDPB have also developed a document on the procedure for the development of informal "Codes of Conduct sessions", with the aim of facilitating discussions concerning draft Codes amongst supervisory authorities, before the formal submission to the EDPB takes place. For the future process of drafting a Code of conduct, knowledge concerning this process may be useful in terms of planning the draft Code development and deciding which supervisory authority may be suited for the SSH GDPR Code of Conduct [13].

Two projects that concern a transnational Code of conduct for research-related activities could serve as relevant sources for insight in the future considerations concerning the competent supervisory authority. These may indicate that a competent supervisory authority has related knowledge of the processing activities that are relevant for an SHH GDPR Code of Conduct:

- European CRO Federation (EUCROF) has developed a GDPR Code of Conduct for contract/clinical research organizations. The French supervisory authorities (CNIL) have been identified as the competent supervisory authority as well as monitoring body for the Code of conduct [14]
- Similarly, BBMRI-ERIC is in the process of developing a GDPR Code of Conduct for Health Research. Their potential findings may be of relevance for other research-related Codes of conduct [14]

2.5 Determining mechanisms

A GDPR Code of Conduct draft shall contain a plan for mechanisms that enable the monitoring body to achieve adequate monitoring of compliance with its provisions [1, 7]. According to the EDPB Guidelines "... all proposed monitoring mechanisms as to how to give effect to adequate monitoring of a Code will need to be clear, suitable, attainable, efficient and enforceable (testable). Code owners will need to set out the rationale and demonstrate why their proposals for monitoring are appropriate and operationally feasible" [7]. Going forward, a draft SSH GDPR Code of Conduct will need to demonstrate how its proposed mechanisms for monitoring compliance are all the above.

The EDPB Guidelines further state that "Mechanisms may include regular audit and reporting requirements, clear and transparent complaint handling and dispute resolution procedures, concrete sanctions and remedies in cases of violations of the Code, as well as policies for reporting breaches of its provisions" [7].

2.6 Identify a Monitoring body

A monitoring body will need to be identified [1, 5, 11]. The Monitoring body will be responsible for monitoring compliance with the Code, and will need to receive accreditation by the competent supervisory authority [5, 11].

The terms for accreditation are outlined in the GDPR Article 41 (2) [5]. The Monitoring body must be able to demonstrate its independence within the SSH environment, its expertise on the subject matter of the Code and demonstrate that its tasks and duties do not result in a conflict of interest. The Monitoring body must have procedures in place that allow it to assess the eligibility of controllers/processors concerned to apply the Code; to monitor controllers'/processors' compliance with the provisions of the Code; and to periodically review its operations. It must also have appropriate structures in place that are transparent to data subjects and the public, and allow it to handle complaints about infringements of the Code or the way the Code is implemented by a controller/processor [5].

2.7 Consult with stakeholders

The GDPR Recital 99 states that when drawing up a Code of conduct, relevant stakeholders should be consulted. The Code owner should have regard to submissions received and views expressed in such consultations [14]. The EDPB Guidelines state that information as to the extent of consultation that has been carried out, must be included in the draft Code submission and "this should [...] outline the level and nature of consultation which took place with their members, other stakeholders and data subjects or associations/bodies representing them" [7, 15].

Where feasible, the consultation process should include data subjects. "Where no consultation has been carried out with regard to relevant and specific stakeholders due to the lack of feasibility, it will be a matter for the Code owner to explain this position" [7]. The requirements according to the GDPR and accompanying guidelines seem to call for a gradual and recurring consultation process. The process must facilitate consultations and ensure the ability to regard the views and expressions of various stakeholders. Simultaneously, it must ensure that documentation requirements are met (see chapter 2.3 above).

Combined, these requirements likely necessitate consultations at several stages. Depending on the opinions provided by stakeholders during consultation, the draft will need to adapt and conclude on topics, needs and concerns that are voiced. This may in turn prompt demand for further consultation with stakeholders, as the draft Code is being developed, specified and refined.

Ensuring that the body or associations responsible for drafting the Code can represent and understand the sector, will likely ensure that the drafting and consultation process progresses effectively. Likewise, ensuring that stakeholders and potential members understand the benefits of an SSH GDPR Code of Conduct, the drafting process and the need to prioritise responding to consultation requests thoroughly, will also benefit the progress of drafting an SSH GDPR Code of Conduct. It can be helpful to set a defined plan for future consultations concerning the different topics and requirements that a draft Code must address.

2.8 Compliance with national legislation

Codes of Conduct must comply with the national laws of countries in which they will apply [7]. This is something to keep in mind, especially since research is one of the sectors where the EU/EEA Member States can provide supplementary regulations according to the GDPR [1].

Code owners must also provide confirmation that a draft Code complies with relevant national legislation [7]. According to EDPB's guidelines, 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" [7]. Since SSH GDPR Codes of Conduct are intended to apply transnationally, such confirmation will require in-depth knowledge of relevant national legislation in various countries. Relevant national legislation should therefore be identified and investigated, and a plan should be made for how compliance with relevant national legislation can be reached.

2.9 The language

The language in which the draft Code is to be submitted to the supervisory authority depends on which competent supervisory authority is to approve the Code [1, 7]. However, no matter what language, the SSH GDOR Code of Conduct should also be presented in English and possibly in all applicable languages within the Code's territory, as it is likely to be a transnational Code within Europe.

3 Suggesting an SSH GDPR Code of Conduct

The report "Draft SSH GDPR Code of Conduct" included suggestions for what an SSH GDPR Code of Conduct might regulate [1]. In this chapter a summary of these suggestions is presented.

Partners have been consulted on these suggestions and were provided an option to make additional suggestions for the purpose of gaining considerable involvement, support and endorsement from the SSH Environment. Results from these consultations are presented in in Chapter 4. What the SSH GDPR Code of Conduct draft shall regulate, must be jointly decided within the SSH Environment [1, 7].

3.1 Broad or narrow scope

When drafting an SSH GDPR Code of Conduct, the SSH environment must determine both the territorial and the material scope of the Code.

How broad the territorial scope of the Code should be will depend on the Codes intended purpose. There are certain advantages to having country-specific Codes. It may be an easier process to both create and implement such a Code without the obstacle of differing national laws and practices. However, the main purpose of the EOSC is to facilitate data sharing, use and reuse within the EU/EEA. Therefore, it would be most expedient for an SSH GDPR Code of Conduct to have a broader territorial scope, encompassing all EU/EEA countries. A Code that ensures equal application of certain provisions of the GDPR within the SSH environment can both enable and simplify the goal of sharing and reusing data across national borders. However, documenting data processing practices more narrowly from participating institutions could serve as a helpful starting point to uncover which common elements could be factored into a wide-ranging Code.

In terms of the material scope of what an SSH Code of Conduct should regulate, there is a wide range of topics to choose from. The scope could be either broad or narrow, and there are advantages and disadvantages related to both alternatives [1].

With the approach of a broad scope, the Code could serve as a comprehensive common framework on how SSH research can comply with all (or many) of the articles in the GDPR. The advantage of such a Code would be that it provides GDPR standards and tools for the entire research process within all branches of humanities and social science research. The main disadvantage, however, would be the enormous amount of work required to complete and draft the Code. In addition, the Code may prove difficult to concretise [1].

The approach of a narrow scope, on the other hand, would allow the SSH community to focus on how research can comply with one (or a few) article(s) in the GDPR, and/or give standards for a smaller part of the research process/area. A huge advantage of narrowing the scope is that it would require less resources to develop and implement the Code. With good planning, the SSH community can select a strategic topic for the Code, and thus ensure that it will be of great benefit to researchers within a relatively short time. Further, it might be possible to later expand to a broader SSH GDPR Code of Conduct or a more comprehensive reference work [1].

3.2 What the SSH GDPR Code of Conduct can regulate

The proposal is to create an SSH GDPR Code of Conduct in Europe concerning the lawful basis of processing personal data for research purposes [1]. When processing personal data, all processing must fulfil the conditions of at least one of the alternatives in the GDPR Article 6 (1). When processing special categories of personal data, the conditions of at least one of the alternatives in the GDPR article 9 (2) must also be met [16, 17]. The lawful bases used for research must be sustainable, to ensure long term and broad data access for further use. Facilitating long term storage and sharing of research data in Europe is an explicit goal of SSHOC, and reusing data created by others holds great promise in research [18]. However, it is likely that large amounts of research data collected in Europe today cannot be reused. It can be argued that an important reason behind this is the lack of a lawful basis for the further processing of personal data.

When collecting and reusing personal data, European research institutions must ensure lawful bases that allow for storing and sharing, not only within their own country, but also across national borders within the EU/EEA-area [19-21]. 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 personal data, while also ensuring that the processing safeguards the rights and freedoms of data subjects. The individual research institution could therefore benefit from specific guidelines in this 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.

Before suggesting which, lawful bases are best suited for an SSH Code of Conduct, a brief description of four lawful bases most used for processing data for research is presented with some of their advantages and disadvantages.

Consent (GDPR art. 6(1) a, and art. 9(2) a)

Consent (GDPR Article 6 (1) letter a, and Article 9 (2) letter a) constitutes a well-functioning lawful basis for processing personal data for research in many cases and is widely used as a lawful basis in the research field. For consent to be valid, certain requirements must be fulfilled. According to the GDPR, consent must be informed, voluntary, specific, unambiguous, documentable and possible to withdraw as easily as it was given [22]. If the data subjects have the competence or capacity to give consent, and are actively participating in research, it is usually an easy task to meet these criteria. Consent is particularly suitable as a lawful basis when data is collected through interviews, questionnaires, or participatory observation. It is also typically used to obtain confidential data from journals and registers, or from occupational groups that have a duty of confidentiality.

A major benefit of using consent as a legal basis is that the GDPR in principle provides the same rules for consent in all European countries. However, this applies if health information, biological and genetic data and criminal offence data are not included in the data material [1]. Another advantage is that the GDPR allows for relatively broad consent in research, through exemptions from the requirements for purpose and storage limitation in Article 5 letter b and e [23]. By forming broad consent, one can facilitate long-term storage and sharing of research data across European countries.

However, in certain situations the requirements for consent will make it disproportionately difficult or impossible to achieve the research aim. For research involving vulnerable people, for example, it is not always possible to ensure that participation is voluntary. Furthermore, the data subjects' right to have their personal data deleted upon withdrawal of consent can present challenges for the implementation of research. It may for one be difficult to identify someone in the dataset sufficiently to find their data. It can also be detrimental to the research if someone withdraws their consent after their information has been included in analyses or publications, especially when the data set is based on few data subjects. Where there are many data subjects, the validity of the research could be affected if there are biases in the sample groups that withdraw. In addition, the requirement of documentation to have a valid consent as legal basis for processing personal data, can also be difficult to fulfil within research. This partly shows why consent is not always the best-suited option for research.

Public interest/scientific purposes (GDPR art. 6(1) e, and art. 9(2) j)

For public interest (GDPR Article 6(1) letter e) to be valid as a lawful basis, it is crucial that "processing is necessary for the performance of a task carried out in the public interest (…)". For the use of scientific purposes (GDPR's Article 9(2) letter j), the processing must be considered necessary for research- or archiving purposes. In addition, the processing must be in line with Article 89(1), and there must be a supplementary lawful basis in place, in Union law or Member State law to which the controller is subject, that determines additional safeguards for the processing [16, 17].

These lawful bases might be considered more flexible than consent, as the data controller has more freedom to select privacy measures that apply to the context and needs of the research [1]. However, the collective measures must sufficiently safeguard the data subject's rights and freedoms. This will require the data controller to conduct and document case-by-case assessments of appropriate safeguards. Research institutions will have to gain oversight over all the applicable data protection measures and assess how the various measures should be combined for each processing. In turn, the institutions can easily implement overly strict measures that will create unnecessary obstacles or fail to secure and document sufficient measures for the conditions in the lawful bases to be met.

Another challenge when using these lawful bases is the requirement for a supplementary lawful basis [1, 17]. The GDPR allows for different laws in different European countries. It is possible that national provisions, which provide conditions for research on personal data, may vary amongst countries in the EU/EEA. This can make it challenging to use a public interest as a lawful basis, especially in research where it is an objective to facilitate sharing and reuse of data across European countries [16, 17].

Legitimate interests (GDPR art. 6(1) f)

A condition in GDPR Article 6(1) letter f 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" [17]. This lawful basis can appear as a more flexible alternative compared to others when processing general categories of research data. However, it might not always be the most suitable option (ICO) [24]. The use of this lawful basis seems to require the data controller to demonstrate that the research is in fact a legitimate interest. The

data controller must also demonstrate that its legitimate interests do not override the rights and freedoms of the data subjects [17]. The data controller is then obliged to perform a balancing test by demonstrating that the controller's legitimate interests are not overriding the interests (i.e., rights and freedoms) of the data subject. This essentially leaves the data controller with the task of extra carefully considering and protecting people's rights and interests for each processing [25].

It may thus be safer for research institutions to instead use public interest as a lawful basis for processing personal data for scientific purposes, pointing out that they are performing a public task [1, 17]. Even though this will require the data controller to carry out a somewhat similar assessment, the use of public interest does not require the demonstration of a legitimate interest. Public interest, with supplementary regulations, often defines research as a public task, and guidelines set in national regulations can give necessary guarantees for the rights and freedoms of the data subject [17].

Publicly available data (GDPR art. 9(2) e)

According to GDPR Article 9(2) letter e, the processing of personal data for research purposes is permitted given that the "processing relates to personal data which are manifestly made public by the data subject " [16].

For this to be an applicable lawful basis for research, one precondition is that the person in question has intended to make the personal data public or has publicly confirmed it, e.g., in an authorized biography, newspaper article or online [1]. Information published on Facebook or other internet forums might not necessarily have 'expected publicness' i.e., the information published in these forums is not necessarily 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 [1].

For some research projects with internet-based sources, it may be reasonable, after a thorough 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 processing, in addition to a basis for processing in the GDPR Article 6 [16, 17].

In addition, the data controller (research institution) is responsible for securing and proving/documenting that this is the case and 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 public [16]. This lawful basis cannot be used for personal information published by a child, a person suffering from dementia or others who do not have the cognitive capacity to understand the consequences of publishing data [16, 23, 26].

The weaknesses of this lawful basis for processing can thus be 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) [1].

A suitable alternative is to obtain consent from data subjects for the processing of personal data they have published about themselves, or personal data published about them by others [16].

3.3 Suggestions for lawful bases suitable for an SSH Code of Conduct

This report recommends the establishment of an SSH Code of Conduct for consent, as well as for public interest/scientific purposes [16, 17]. These lawful bases seem to be the most frequently used for research purposes and can be argued to have greatest benefits compared to disadvantages and are hence suitable for an SSH Code of Conduct.

As outlined above, there are some disadvantages associated with these provisions when used for processing personal data for research purposes [16, 17]. However, based on the perception that these provisions are best suited for research, it can be argued that institutions can thus benefit from Codes which will help in navigating these disadvantages.

As for consent, it may be demanding for research institutions to understand and operationalize the consent requirements in the GDPR, which in turn can prevent research data from being shared and reused [16, 17]. The research institutions could therefore benefit from specific guidelines in this area [1]. For one, the Code could serve as a guide to obtaining consent that is unambiguous, freely given and explicit. This will benefit research that includes vulnerable data subjects. Another suggestion is to create a Code that details how to design an information letter to obtain broad consent that also ensures that the conditions for informed consent are met [1].

Potential obstacles may present themselves as European countries may provide stricter national rules for consent for the processing of health data, genetic and biological data and personal information about criminal convictions and offenses. When preparing a common European SSH GDPR Code of Conduct for consent in research, differences in national law between countries in these areas must be identified [1].

As for public interest/scientific purposes, research institutions could benefit from specific guidelines on how to apply these provisions to research without invoking too strict or too lenient measures for their conditions to be fulfilled. One of the challenges that institutions may face when using these lawful bases in research, is determining what information should be given to the data subjects. It can be a difficult balancing act for institutions to figure out how information can be designed to both provide the research with the necessary conditions while at the same time facilitating the exercise of the data subject's rights. As a helpful measure to facilitate this task, this report suggests the design of a common template for information used by researchers across the EU/EEA. This could help facilitate long-term storage and sharing of research data, whether the information is given individually according to Article 13 and 14, or collectively according to Article 14(5) letter b [16, 19, 20].

Further, it can be difficult to gain overview of all the measures that can be used to protect the data subject's rights and freedoms. Hence, the European research sector could cooperate to create an

overview of such privacy measures. Such an overview can also be the subject for an SSH Code of Conduct [1].

A major challenge in using public interest/scientific purposes for research across European borders is the requirement of a supplementary national lawful basis [16, 17]. This could make it difficult to share research data where national laws impose unequal privacy measures. One way to account for this may be to have an overview of privacy measures that specifies where such measures are defined as mandatory, by mapping national supplementary lawful bases. Such an overview could simultaneously make it clear to European authorities that one of the purposes of the GDPR, that is to simplify and harmonize the rules for research and facilitate transnational research collaboration in Europe, is not entirely being achieved. In addition, the supplementary lawful basis may also be established in Union law. Therefore, it is in turn possible for the EU to create common rules for how research can meet the conditions in the GDPR Article 6(1) letter e and Article 9(2) letter j. An SSH Code of Conduct can thus help shed light on the need for such common rules.

It is also important to note that the matter of what the Code can regulate may be affected by the previously outlined terms and conditions that must be met for a Code to be approved. Also, as previously mentioned, what the SSH GDPR Code of Conduct draft shall regulate must be jointly decided within the SSH Environment. Thus, further discussions on when and how the Code should be written and what it should regulate are needed. In chapter 6 of this report, suggestions are presented on how and by whom this should be further discussed.

4 Consulting partners and a supervisory authority

The main aim of establishing an SSH GDPR Code of Conduct is to facilitate easier and harmonized application of the GDPR within the SSH sector. The goal (besides implementing the GDPR) is to reassure data producing institutions how the rules is understood and applied in SSH research. The aim is to contribute to harmonization (equal use / understanding of the rules) meaning that data can be collected, shared and reused on equal terms, which in turn facilitates cross country research and data sharing as well as long-term storage.

To establish such a Code, one of the clear legal requirements is to document the needs, involvement and support of the sector. The involvement of the sector is done by identifying and consulting relevant stakeholders for an SSH GDPR Code of Conduct. In this context, stakeholders can be defined as all parties that can contribute to, or be affected by, an SSH GDPR Code of Conduct. At this stage, consulting all parties that are possibly affected or may have insights is premature. In chapter 5 of this report, a stakeholder analysis is presented.

Thus, at the first stage partners have been consulted by answering ten questions. The aim of the partners' contribution was to get considerable involvement, support and endorsement from the SSH Environment. In addition, a supervisory authority was asked whether the terms in Article 40 of the GDPR were correctly interpreted and to provide more guidance on how to interpret them. An overview of the questions asked, and detailed answers given from partners, is presented in Appendices 1 and 2.

In chapter 4.1, the answers are summarised and analysed. Recommendations for further work on establishing an SSH GDPR Code of Conduct will be presented in chapter 4.2.

4.1 Analysis of legal terms and input from partners

According to EDPB Guidelines 1/2019 on Codes of Conduct, supporting documentation should be attached to underpin every draft Code of Conduct submitted to a supervisory authority. Sufficient documentation must be gathered in further work, to demonstrate the fulfilment of such requirements.

It will also be necessary to further analyse the nature and extent of documentation required to make an SSH GDPR Code of Conduct draft admissible. The national supervisory authorities may be able to provide guidance on this matter, in addition to EDPBs Guidelines [7]. However, given that very few GDPR Codes of Conduct have been drafted and approved[1], as pointed out by the Norwegian Data Protection Authority,

[1] See for instance details about the EU Cloud Code of Conduct: https://eucoc.cloud/en/detail/the-eu-cloud-code-of-conduct-becomes-first-gdpr-code-of-conduct-to-receive-green-light-from-data-protection-authorities

it may be difficult to give comprehensive feedback beyond the general information that is described on its website (https://www.datatilsynet.no/). Guidelines on which documentation that will be required to create a GDPR Code of Conduct will therefore become apparent as more GDPR Codes of Conduct are being developed.

As mentioned earlier, an SSH GDPR Code of Conduct must be established based on actual needs of the SSH sector. Such a Code may benefit the SSH sector in several ways by:

- contributing to the standardisation and harmonisation of the application of the GDPR within the SSH research area, according to ESS ERIC.
- providing an appropriate safeguard and routines that promote and ensure GDPR compliance, according to DARIAH ERIC.
- increasing efficiency and simplifying workflows, according to CLARIN ERIC.
- helping to provide access to and handle personal data without unnecessary obstacles, according to CLARIN ERIC.
- providing an authoritative reference and insurance for data subjects, controllers, and processors, according to DARIAH ERIC. As pointed out by CLARIN ERIC, this could for example be to provide authoritative guidance on what "appropriate safeguards for the rights and freedoms of the data subject", as required in research context by Article 89 of the GDPR, will entail.
- ensuring reputational gain that will benefit the sector as a whole and provide impetus for continued work on maintaining and elaborating the SHH GDPR Code of Conduct, according to ESS ERIC.

An assessment must be made to determine which body should lead the initiative for drafting an SSH GDPR Code of Conduct, based on the criteria and guidelines as presented in chapter 2.1 of this report. According to ESS ERIC, this assessment might consider whether an appropriate representative organisation or body could be an umbrella organisation such as European alliance for social sciences and humanities (EASSH). Further, DARIAH ERIC suggests a coalition of SSH ERICs, a future SSH cluster, or a group including legal experts and researchers with solid knowledge of legal and ethical issues. According to DARIAH ERIC, cultural institutions such as Europeana or Archive Portal Europe could possibly bring contributions to such a group. CLARIN ERIC suggests that the primary responsibility should be with organisations that perform data collection tasks and carry out research agendas. European/international bodies in which research performing organisations collaborate and coordinate policies, should be in the lead. They mention the European University Association, Science Europe, or League of European Research Universities.

Regarding the territorial scope of the Code, the continued work should preferably be based on the ambition to create an SSH GDPR Code of Conduct for all European or EU/EEA countries in which the GDPR applies. This is supported by all partners. In addition, ESS ERIC mentions that the possibility of including countries for which an adequacy decision is granted should also be considered.

In the continued work on the material scope of an SSH GDPR Code of Conduct, one needs to decide whether a narrow scope is the preferred approach. A narrow scope is supported by ESS ERIC and CESSDA ERIC. Neither DARIAH ERIC nor CLARIN ERIC explicitly express their opinion on a narrow scope.

Further work on the material scope is also needed to define more precisely what the SSH GDPR Code of Conduct should regulate, and if it applies to the SSH environment in general or certain parts of the environment. DARIAH ERIC and CESSDA ERIC support the proposal in the report "Draft SSH GDPR Code of Conduct" and in the current initiative for an SSH Code of Conduct for a Code that deals with lawful bases. In addition, ESS ERIC suggests that the content could perhaps address international transfers of personal data, and DARIAH ERIC mentions GDPR research exceptions and points out that further discussion is needed on whether the Code should also address more ethical concerns. CLARIN ERIC stated that a Code should attempt to cover the processing of personal data for research purposes regardless of who the data controllers, processors, or involved parties are. In addition, CESSDA ERIC mentions that data archives should be covered. Also, universities, research institutions as well as research infrastructures with Eric and other legal statutes should be covered, according to ESS ERIC. CLARIN ERIC also noted that the preferred legal basis for research purposes, based on their experiences, varies from one country to another and these differences can be hard to harmonize in one common SSH GDPR Code of Conduct. How these differences are to be resolved, must be subject to further discussions.

In the future work on identifying a monitoring body, it is important to acknowledge that the requirements for a monitoring body will depend on the SSH GDPR Code of Conduct itself, the traits of the sector and the related data processing risks. The monitoring body cannot have conflicts of interest when carrying out its tasks. ESS ERIC mentions that EASS or the EOSC Association could be considered. CLARIN ERIC also refers to the organizations they suggested as representative bodies for this role (European University Association, Science Europe or League of European Research). According to DARIAH ERIC, an advisory board of representatives from expert groups amongst the SSH ERICs and other stakeholders may be in the best position to monitor a Code. DARIAH ERIC mentions one should perhaps investigate the possibility of the monitoring body not being a single institution and not being based in a single country. One should also attempt to harvest experiences from BBMRI ERIC concerning a monitoring body, as addressed by ESS ERIC. In due time, the mechanisms that will enable the suggested monitoring body to carry out its monitoring functions must be elaborated on.

Work on identifying the competent supervisory authority will need to continue [6, 27]. This will depend on the territorial scope of the Code. The parties/countries in which the SHH GDPR Code of Conduct is intended to apply, will determine possible alternatives. If the monitoring body has a headquarter in a specific country, this could be the starting point for identifying the Supervisory Authority, as mentioned by ESS ERIC. But in the case suggested by DARIAH ERIC, where the monitoring body is not necessarily based in one country, this criterion would not be adequate. The location of the Code owner's headquarters may also be an appropriate criterion. In addition, ESS ERIC mentions that the relationship with the ICO/UK should be determined.

If any of the potentially competent supervisory authorities, depending on the territorial scope of the Code, have developed initiatives for a specific field, this could also constitute a relevant factor in determining the competent supervisory authority. There are at least two ongoing projects concerning GDPR Codes of Conduct in research-related fields that may give useful insights, as mentioned in chapter 2.4, not only in terms of the general process of determining the competent supervisory authority, but also in terms of indicating that certain supervisory authorities already have specific initiatives developed concerning research in general.

Ensuring compliance with national legislation will require both a clearly defined territorial scope as well as a clearer content in terms of specific regulations and the material scope of the SSH GDPR Code of Conduct. Once these factors are established, a plan should be made for ensuring compliance with national legislation. Involving stakeholders at a national level may give particularly valuable insight concerning this requirement, but it is important to stress that compliance with national legislation will likely need quality assurance or other well-planned procedures to be successful. The work of identifying when, how and who to carry out this compliance check will need to be continued.

Meeting language requirements means that the Code must be submitted in the language of the competent supervisory authority, as well as in English. Although it is a factor to consider when deciding or identifying the competent supervising authority, language seems like a secondary requirement that should be met based on the outcome of other considerations. However, when scheduling a timeframe for a Code of Conduct process, one should consider the need to appropriately translate the draft.

Appropriate stakeholder involvement must permeate all stages of the process and will be a crucial element in shaping a potential SSH GDPR Code of Conduct. ESS ERIC mentions that future consultations within the SSH Environment might include the possibility of voicing opinions at stakeholder events, as well as written consultations. According to DARIAH ERIC, the possibility to comment on a written draft Code through crowdsourcing and annotation procedures should be considered, perhaps at a later stage. The leadership level of stakeholders could, according to DARIAH ERIC, be addressed during the consultation, explicitly encouraging involvement of their expert groups, or as mentioned by ESS ERIC, persons with data protection responsibilities.

ESS ERIC mentions that LERU (League of European research universities) and EASSH (SSH association) might be included as key stakeholders/representative bodies. Further, DARIAH ERIC suggested that DARIAH Working Groups Ethics and Legality in the Digital Arts and Humanities (ELDAH) and Research data management (RDM) should also be included as stakeholders in future consultations. Finally, according to CLARIN ERIC, ethics committees of research infrastructures and the ERIC Forum should also be included. One such possible committee could be CLARIN Legal and Ethical Committee (CLIC).

It may be useful to consult organizations that have previous experience considering or establishing GDPR Codes of Conduct. According to ESS ERIC and CLARIN ERIC, BBMRI ERIC and ENSOMAR may have valuable input based on their experiences, with the creation of a Code of Conduct. Other initiatives such as EUCROF may be able to provide valuable knowledge and insights on how to handle the procedural terms required for the establishment of a GDPR Code of Conduct. As the supervisory authority mentions, "The Code" by the Norwegian Directorate of Health, may also be able to provide such valuable knowledge and insights.

4.2 Recommendations

Amongst the legal requirements that must be met to make a draft Code admissible, many will depend on how the SSH sector decides to define the processing scope (the categories of processors, controllers and processing activities within the SHH environment concerned), as well as the territorial scope of the SSH GDPR Code of Conduct. This decision must be based on thorough investigation of the needs of the

SSH Environment. It will be important to identify a suitable representative body or organization that can coordinate and act on behalf of the sector to advance the work on a draft Code of conduct and assess which bodies can act as Code owners.

In further work towards an SSH GDPR Code of Conduct, given the scope of this report mentioned in Chapter 1, the recommendation is to initially focus on the following steps and requirements:

- Consulting the sector and identifying and documenting its specific needs, e.g., to facilitate cross-border data sharing, seamless access, reuse, and long-term storage of research data
- Finding and agreeing on an organization or body that can represent the SSH Environment
- Determining the potential processing scope and territorial scope of the SSH GDPR Code of Conduct

Once these steps are taken, further work on fulfilling the requirements for a draft Code can be continued more efficiently. Additional work that will follow includes:

- Further developing the stakeholder analysis
- Analysing what an SSH GDPR Code of Conduct should encompass, in further detail
- Identifying and designating the Monitoring body
- Determining mechanisms to ensure transparency and monitoring compliance
- Determining the competent Supervisory authority
- Ensuring compliance with national legislation
- Meeting the language requirements for a draft Code

According to Recital 99 of the GDPR, associations and other bodies representing categories of controllers or processors should consult relevant stakeholders in the Development of Codes of Conduct, including data subjects where feasible, and have regard to submissions received and views expressed in response to such consultations. This will also ensure that the scope of an SSH GDPR Code of Conduct will successfully meet the needs of the SSH sector. Furthermore, the whole process must be adequately documented, taking into consideration the overarching needs to supplement the explanatory statement with supporting documents.

5 Stakeholder analysis

As mentioned in Chapter 1.3, relevant stakeholders must be consulted if a draft Code of Conduct is to be developed [7]. This means that relevant stakeholders for an SSH GDPR Code of Conduct must be identified and contacted. In this context, stakeholders can be defined as all parties that can contribute to, or be affected by, an SSH GDPR Code of Conduct. At this stage, consulting all parties that possibly are affected or may have insights is premature.

The report "Draft SSH GDPR Code of Conduct" identified relevant stakeholders for an SSH GDPR Code of Conduct, by creating a stakeholder analysis represented in Chapter 6. It was stressed that this stakeholder analysis only represented a starting point and should be further developed in upcoming work [7] [1]. The report identified the following stakeholders: researchers, research institutions, data subjects (participants in research projects), supervisory authorities, EDPB, data archives, EOSC, CESSDA ERIC, NSD, BBMRI ERIC and other institutions with experiences creating Codes of Conduct, Authorities, such as Ministries of Education, interest groups for participants, register managers and the EU commission [1].

Therefore, an expanded stakeholder analysis has been made. This can be read in Appendix 3. The parties have been identified based on consultation with relevant stakeholders [1]. It is important to stress that this stakeholder analysis is not exhaustive and should be further developed to include all relevant parties that are necessary to consult to make a draft Code of Conduct admissible.

6 Conclusion

This report provides a set of recommendations on how to establish an SSH GDPR Code of Conduct draft. The legal terms to make a draft Code admissible have been explained and further investigated, and suggestions on what an SSH GDPR Code of Conduct can regulate have been presented.

Involvement of the SSH environment is of utmost importance in the process of establishing an SSH GDPR Code of Conduct. A questionnaire was developed based on the legal terms for an SSH GDPR Code of Conduct and sent to partners and one supervisory authority. Answers were provided by four partners and one supervisory authority. This was analysed, and did provide input on the need, purpose, and scope of such a Code, what it should regulate and who should be involved. Based on the inputs, an extended stakeholder analysis has been developed. The elaboration on content of legal requirements to get a draft Code of Conduct admissible, the questionnaire and answers given constitutes the foundation of recommendations given in this report.

The consultation of stakeholders so far represents a starting point of bringing the initiative of an SSH GDPR Code of Conduct out to the SSH sector. In the further process of developing the Code, more extensive contributions from the sector must be organized.

The contribution in this report aims to facilitate the work of establishing an SSH GDPR Code of Conduct. A tentative framework has been suggested for the process of developing a draft SSH GDPR Code of Conduct, identifying which terms should be addressed first, and how.

It is recommended that the work of establishing an SSH GDPR Code of Conduct is continued, for the benefit of the EOSC, the European research environment, data sharing and society at large. A future roadmap for establishing an SSH GDPR Code of Conduct could be to plan the next steps as a proposal under a new Horizon Europe call.

7 References

1. Ina Nepstad, Inga Brautaset, Mathilde Steinsvåg Hansen, Tore A. K. Fjeldsbø, Siri Tenden, Marita Ådnanes Helleland, Christopher Ongre Autzen, Ingvild Eide Graff, Marianne Høgetveit Myhren, & Vigdis Namtvedt Kvalheim. (2021). 5.8 Draft SSH GDPR Code of Conduct (v1.0). Zenodo. https://doi.org/10.5281/zenodo.5181223.
2. Maurizio Sanesi, Lea Sztuk Haahr, Mathilde Steinsvåg Hansen, Ina Nepstad, Belinda Gloppen Helle, Marianne Høgetveit Myhren, Marita Ådnanes Helleland, Tore Andre Kjetland, Ingvild Eide Graff, & Vigdis Kvalheim. (2021). D5.7 Report on the impact of the GDPR and its implications for EOSC (1.0). Zenodo. https://doi.org/10.5281/zenodo.4723645.
3. Hansen, M.S., et al., *D5.19 Report on Stakeholder workshop about SSH Code of Conduct (1.0).* Zenodo, 2021: p. 1-23.
4. *European Commission. Two years of the GDPR: Questions and answers*. 2020 [cited 2020 March]; Available from: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_1166.
5. GDPR, *Art. 41. Monitoring of approved codes of conduct*. 2018.
6. GDPR, *Art. 40. Codes of conduct*. 2018.
7. EDPB, *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679*. 2019. p. 1-30.
8. Datatilsynet. *Kva er ei atferdsnorm (bransjenorm)*. 2018 [cited 2021 October]; Available from: https://www.datatilsynet.no/regelverk-og-verktoy/atferdsnorm/korleis-lage-atferdsnorm/kva-er-ei-atferdsnorm/.
9. Datatilsynet. *Korleis gå fram for å lage ei atferdsnorm?* 2018 [cited 2021 October]; Available from: https://www.datatilsynet.no/regelverk-og-verktoy/atferdsnorm/korleis-lage-atferdsnorm/korleis-lage-ei-bransjenorm/.
10. WP8, - *Governance/ Sustainability/ Quality Assurance [Months: 1-40], CNR, CESSDA ERIC, ESS ERIC, SHARE ERIC, CLARIN ERIC, DARIAH ERIC, LIBER, KNAW, TRUST-IT*. 2021. p. 60-81.
11. GDPR, *Art. 57. Tasks*. 2018.
12. *European Commision. Working Party on the Protection of Individualswith regard to the Processing of Personal Data. Judging industry self-regulation: when does it make a meaningful contribution to the level of data protection in a third country?* 1998. p. 2-3.
13. EDPB, *Annual Report 2020. Adopted EDPB Documenton the procedure for the development of informal "Codes of Conduct sessions"*. 2020. p. 1-9.
14. BBMRI-ERIC. *A Code of Conduct for Health Research*. 2021 [cited 2021 October]; Available from: https://code-of-conduct-for-health-research.eu/.
15. GDPR, *Recital 99. Consultation of Stakeholders and Data Subjects in the Development of Codes of Conduct**. 2018.
16. GDPR, *Art. 9. Processing of special categories of personal data*. 2018.
17. GDPR, *Art. 6. Lawfulness of processing*. 2018.
18. *European Commission. European Open Science Cloud (EOSC) - What the cloud is, how it was developed and being implemented* 2021 [cited 2021 October]; Available from: https://ec.europa.eu/info/research-and-innovation/strategy/strategy-2020-2024/our-digital-future/open-science/european-open-science-cloud-eosc_en.
19. GDPR, *Art. 14. Information to be provided where personal data have not been obtained from the data subject*. 2018.

20. GDPR, *Art. 13 Information to be provided where personal data are collected from the data subject*. 2018.
21. GDPR, *Art. 12 Transparent information, communication and modalities for the exercise of the rights of the data subject*. 2018.
22. GDPR, *Art. 7. Conditions for consent*. 2018.
23. GDPR, *Art. 5. Principles relating to processing of personal data*. 2018.
24. ICO. *Legitimate interests* 2021 [cited 2021 November]; Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/.
25. GDPR, *Art. 24. Responsibility of the controller*. 2018.
26. GDPR, *Art. 8. Conditions applicable to child's consent in relation to information society services*. 2018.
27. GDPR, *Art. 55 Competence*. 2018.

Appendix 1: Questions

Who to represent the SSH Environment?

In order to get input on how to meet the requirement of finding a body that could represent the SSH Environment, the partners received the following question:

- Which organization(s) would be able/appropriate to represent the SSH research environment, and should thus be given the mandate to draft the SSH GDPR Code of Conduct? How should this be determined?

The Norwegian Data Protection Authority received the following questions:

- Is the interpretation of the term appropriate? If not, how should it be interpreted?
- How can it be decided who gets the mandate to create/ draft the Code of Conduct? Which criteria do you mean are relevant to identify an appropriate representative for the SSH Environment and to determine if they have the proper competence.

Explanatory statement and supporting documents

In order to get input on how to meet the requirement of explanatory statement and supporting documents, the partners consulted received the following question:

- What are the most important benefits that may result from a GDPR Code of Conduct, for research and for the research environment?

The Norwegian Data Protection Authority received the following question:

- Is the interpretation of the term appropriate, and if not, how should it be interpreted.
- How should the need for an SSH GDPR Code of Conduct be documented? Including, its scope and purpose, and how the Code will facilitate an effective use of GDPR.
- How comprehensive must the documentation be? Are there specific details you think are necessary to document?

Processing and territorial scope of the SSH GDPR Code of Conduct

In order to get input on how to meet the requirement of defining the processing and territorial scope, the partners consulted received the following question:

- What should be the territorial scope of an SSH GDPR Code of Conduct?
  All European countries? Only countries in the EU/EEA? Or fewer countries? Then which criteria should be used to narrow the area?
- Within the SSH Environment, which parties and processing activities should be covered by a GDPR Code of Conduct (referred to as" processing scope" of a Code)?

The Norwegian Data Protection Authority received the following question:

- Is the interpretation of the term appropriate, and if not, how should it be interpreted?

- What should be assessed before determining the territorial scope? How will the scope affect the necessity of documentation?
- Does the scope need to be justified? And is it necessary to document if stakeholders have been consulted?
- In EDPBs guidelines it is mentioned that one must determine a "processing scope". We kindly ask for guidance on how this should be interpreted and how it must be documented.
- What are the demands for documentations in relation to territorial scope? Is it sufficient to state that the Code will, for instance, apply to all EU/EEA countries? Or will it be necessary with a broader explanation?

Supervisory authority

In order to get input on how to meet the requirement of defining the competent Supervisory authority, the partners consulted received the following question:

- Which criteria should be used to determine which supervisory authority/authorities that is competent to assess and approve the SSH GDPR Code of Conduct? Should the SSH environment e.g., look to the country/ countries where:

- Most of processing activities take place, most of the data subjects are located, the organization(s) representing the SSH research environment are located, the monitoring body has its headquarter?

The Norwegian Data Protection Authority received the following question:

- Is the interpretation of the term appropriate, and if not, how should it be interpreted?
- In EDPBs guidelines there are given some examples on different criteria that may help the Code owner to locate the competent supervisory authority. An SSH GDPR Code of Conduct is likely to have an international scope, where the controllers, processors and data subjects are located throughout Europe, it can be assumed that the criteria will be: The location of the Code owner`s headquarters, and the location of the proposed monitoring body`s headquarters (assuming this is a body in one country). Do you agree with this assessment?
- Will this be affected if the monitoring body is an association, including different companies located in different countries?
- Do you see any further factors that should be considered in this assessment?

Determine mechanisms

In order to get input on how to meet the requirement of determining mechanisms for the Monitoring body, the Norwegian Data Protection Authority received the following question:

- Is the interpretation of the term appropriate, and if not, how should it be interpreted?

Identify a Monitoring body

In order to get input on how to meet the requirement of identifying a Monitoring body, the partners consulted received the following question:

- Which organization(s) would be appropriate to monitor the SSH GDPR Code of Conduct? Given the criteria: independent, expertise on the subject matter of the Code, be able to establish the mechanisms necessary to perform its tasks and demonstrate that its tasks and duties do not result in a conflict of interest. How should this decision be taken, in your opinion?

The Norwegian Data Protection Authority received the following question:

- Is the interpretation of the term appropriate, and if not, how should it be interpreted.
- Do you still consider it as uncertain that such a monitoring body must exist, or has this been determined?
- Can you advise on which type of parties should monitor an SSH GDPR Code of Conduct?
- What should be emphasized to determine which candidates are able to perform the task as assigned to a monitoring body?

Consult with stakeholders

In order to get input on how to meet the requirement of consulting stakeholders, the partners consulted received the following question:

- In section 6 of the report "Draft SSH GDPR Code of Conduct", the authors identified some stakeholders that can be relevant to include/Consult. This analysis is provided in Appendix 3. Please suggest further stakeholders that should be contacted in the process, and for what.
- How should consultations with relevant stakeholders be performed? Who should be contacted (which organizations, at which level)? On what subjects/questions should they be consulted? In what form should they be able to give their feedback?

The Norwegian Data Protection Authority received the following question:

- Is the interpretation of the term appropriate, and if not, how should it be interpreted.
- How should stakeholders be identified and consulted? And how to document that proper consultation has been performed with stakeholders.
- Do you advise on any specify number of consultations and or/stakeholders?
- How do you suggest that stakeholders should be identified?
- At which level should the stakeholders be consulted?
- About which topics do you mean the stakeholders must be consulted?
- How should the stakeholders be able to provide their input?

Compliance with national legislation

In order to get input on how to meet the requirement of compliance with national legislation, the Norwegian Data Protection Authority received the following question:

- Is the interpretation of the term appropriate, and if not, how should it be interpreted.
- In your opinion, are there any obstacles in relation to the term stating that an international Code of Conduct must adhere to appropriate national legislation?
- Should this term be taken into account when defining the scope and/or purpose of the Code of Conduct?

The language of the SSH GDPR Code of Conduct draft

In order to get input on how to meet the requirement of language in the SSH GDPR Code of Conduct Draft, the Norwegian Data Protection Authority received the following question:

- Is the interpretation of the term appropriate, and if not, how should it be interpreted.

Suggested content - Broad or narrow scope

In order to get input on whether an SSH GDPR Code of Conduct should have a broad or a narrow scope in terms of content, the partners consulted received the following question:

- In the report "Draft SSH GDPR Code of Conduct", the authors suggests that a first version of an SSH GDPR Code of Conduct should have a narrow scope and proposes that the lawful basis for processing personal data for research purposes may be the subject for an SSH Code of Conduct.
- Do you agree on a narrow scope as a starting point?
- If yes, why?
- If no, why not? Then, how broad should the scope of an SSH Code of Conduct be?

Content

In order to get input on what an SSH GDPR Code of Conduct should contain, the partners consulted received the following question:

- Do you agree on the authors' proposal for what an SSH Code of Conduct can contain?
  If yes, why?
  If no, why not?
- Do you have other suggestions for what an SSH Code of Conduct should contain?
- What are the most important benefits that may result from a GDPR Code of Conduct, for research and for the research environment?

Appendix 2: Stakeholder analysis

Stakeholder	How can they influence the work and what can they contribute to	Can they be affected by an SSH GDPR Code of Conduct and how?
SHARE ERIC, DARIAH ERIC, ESS ERIC, CESSDA ERIC, CLARIN ERIC, CNR	To facilitate the creation of an SSH GDPR Code of Conduct	Responsibilities when processing personal data, set in GDPR can be fulfilled.
The Norwegian Data Protection Authority ("Datatilsynet").	They have the mandate to provide guidance on how to comply with the GDPR, they are to approve Code of Conduct and encourage the creation of Codes of Conduct. They can provide guidance on if the understanding of the terms in GDPR article 40 and 41 is correct, and possibly to provide further guidance on how to interpret them.	A Code of Conduct can lead to specific needs within the SSH Sector. They will have knowledge of the SSH GDPR Code of Conduct and can provide guidance to the SSH environment on the existence of such a Code.
The Norwegian Directorate of Health ("Helsedirektoratet")	They are creating «The Code» ("Normen"). This is an industry Code of Conduct for information security and privacy that is prepared and managed by organisations and companies in the Norwegian health sector. While doing so they made assessments of whether it was possible to make «The Code» a GDPR Code of Conduct.	They will have knowledge of the SSH GDPR Code of Conduct and can provide guidance to the SSH environment on the existence of such a Code. Experiences can also be shared between the Code owners.
Umbrella organisation, such as EASSH	Can contribute as a body or organisation representing the SSH research environment, and the mandate to develop a draft Code.	

	EASSH can be a monitoring body.	
The EOSC Association. The experience of BBMRI in this regard would be useful.	Can act as a monitoring body.	
Research universities and research institutes as well as research infrastructures with ERIC and other legal statutes		Can be subject to the Code.
LERU (League of European research universities)	Can act as representative bodies, key stakeholders.	
Legal experts with a background in research processes and ethics as well as researchers with a solid knowledge of legal and ethical issues	In order to minimize miscommunication and ensure that the result meets not only the legal and ethical requirements but also the needs of the community	
SSH ERICs	A coalition of SSH ERICs at the crossroad between infrastructures and research seems an appropriate organisation to represent the SSH environment. Might be in position to competently monitor a Code of Conduct.	
Cultural institutions (such as Europeana or Archive Portal Europe)	Can be interesting when assessing appropriate organisations to represent the SSH environment. Might be in position to competently monitor a Code of Conduct	
the ELDAH Working Group, https://www.dariah.eu/activities/working-groups/ethics-and-legality-in-the-digital-arts-and-humanities-eldah/	Can have necessary input, experiences and suggestions	
the RDM Working Group, https://www.dariah.eu/activities/working-groups/research-data-management/	Can have necessary input, experiences and suggestions.	

Data related organisations (archives, RIs, universities, institutes, etc.		
SSH ERICs or SSHOC MoU organisations	Can act as representative bodies. Might be in position to competently monitor a Code of Conduct.	
European/international bodies in which research performing organisations collaborate and coordinate policies should be in the lead. E.g., European University Association (https://eua.eu), Science Europe (http://www.scienceeurope.org), League of European Research (https://www.leru.org).	Can act as representative bodies. Might be in position to competently monitor a Code of Conduct.	
SSHOC 1st Tier	Might be in position to competently monitor a Code of Conduct.	
Ethical committees of research infrastructures and ERIC Forum. All RIs.		