Deliverable Number: 6.2

Deliverable Title: Guidelines on the use of social media data in survey research

Work Package 6: New forms of data: legal, ethical and quality matters

Deliverable type: Report

Dissemination status: Public

Submitted by: CESSDA, NSD

Authors: Sunniva Hagen (CESSDA, NSD) Øyvind Straume (CESSDA, NSD), Elisabeth Lea Bishop (CESSDA, UKDA), Martin Vavra (CESSDA, CSDA), Michal Koščík (CESSDA, CSDA), Janez Štebe (CESSDA, ADP), Lorna Ryan (ESS, CITY), Linn-Merethe Rød (CESSDA, NSD), Eva J. B. Payne (CESSDA, NSD), Anne-Mette Somby (CESSDA, NSD), Hervé L’Hours (CESSDA, UKDA), Tom Emery (GGP), Tomas Cizek (CESSDA, CSDA), Jindrich Krejci (CESSDA, CSDA), Marianne Høgetveit Myhren (CESSDA, NSD). Curtis Jessop (NatCen Social Research).

Date submitted: July 2019

Legal disclaimer: This does not constitute or should not be construed as legal advice and/or guidance

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 654221.
SERISS (Synergies for Europe’s Research Infrastructures in the Social Sciences) aims to exploit synergies, foster collaboration and develop shared standards between Europe’s social science infrastructures in order to better equip these infrastructures to play a major role in addressing Europe’s grand societal challenges and ensure that European policymaking is built on a solid base of the highest-quality socio-economic evidence.

The four year project (2015-19) is a collaboration between the three leading European Research Infrastructures in the social sciences – the European Social Survey (ESS ERIC), the Survey for Health Aging and Retirement in Europe (SHARE ERIC) and the Consortium of European Social Science Data Archives (CESSDA AS) – and organisations representing the Generations and Gender Programme (GGP), European Values Study (EVS) and the WageIndicator Survey.

Work focuses on three key areas: Addressing key challenges for cross-national data collection, breaking down barriers between social science infrastructures and embracing the future of the social sciences.

# Contents

1 Introduction  
2 Questions and Answers  

## Research Design and Data Collection

<table>
<thead>
<tr>
<th>Question</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>When do I need to think about the legality and ethics of social media data linkage?</td>
<td>4</td>
</tr>
<tr>
<td>What is considered personal data in linked data sets?</td>
<td>4</td>
</tr>
<tr>
<td>What information do I need to give to participants?</td>
<td>5</td>
</tr>
<tr>
<td>Do I always have to give information when linking social media data?</td>
<td>5</td>
</tr>
<tr>
<td>Timing of information to data subjects?</td>
<td>6</td>
</tr>
<tr>
<td>What is the difference between legal and ethical consent?</td>
<td>6</td>
</tr>
<tr>
<td>What is granular consent and how could it be applied?</td>
<td>6</td>
</tr>
<tr>
<td>What is a data management plan?</td>
<td>8</td>
</tr>
</tbody>
</table>

## Data Processing

<table>
<thead>
<tr>
<th>Question</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>When am I processing personal data?</td>
<td>8</td>
</tr>
<tr>
<td>What are relevant legal bases for processing social media data?</td>
<td>9</td>
</tr>
</tbody>
</table>

## Archiving and Sharing

<table>
<thead>
<tr>
<th>Question</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Why deposit research data?</td>
<td>10</td>
</tr>
<tr>
<td>What are the key legal and ethical challenges when preserving social media data?</td>
<td>10</td>
</tr>
<tr>
<td>Why is it important to consider social media platforms’ terms and conditions?</td>
<td>11</td>
</tr>
<tr>
<td>What about copyright infringement?</td>
<td>11</td>
</tr>
<tr>
<td>Has consent been obtained?</td>
<td>12</td>
</tr>
<tr>
<td>When is social media data anonymous?</td>
<td>12</td>
</tr>
<tr>
<td>Can direct quotes be published as part of a research paper/report?</td>
<td>13</td>
</tr>
<tr>
<td>What about research integrity?</td>
<td>14</td>
</tr>
<tr>
<td>Is there any infrastructure for archiving social media data?</td>
<td>14</td>
</tr>
<tr>
<td>How can social media data be deposited within a data archive?</td>
<td>15</td>
</tr>
<tr>
<td>How can I prepare my data for archiving and sharing?</td>
<td>15</td>
</tr>
</tbody>
</table>

## Definitions

<table>
<thead>
<tr>
<th>Appendix</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appendix A: Example Information Letter</td>
<td>20</td>
</tr>
<tr>
<td>Appendix B: Example Information Letter</td>
<td>23</td>
</tr>
<tr>
<td>Appendix C: Example Twitter Consent Module</td>
<td>26</td>
</tr>
</tbody>
</table>

## References

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>References</td>
<td>27</td>
</tr>
</tbody>
</table>
1 Introduction

Large amounts of digital data are being generated every day from sources such as Facebook, Instagram and Twitter. Whilst Twitter has around 500 million tweets sent each day, Facebook had 2.38 billion monthly active users as of the first quarter of 2019.\(^1\) The social media data\(^2\) that are available offer a great research potential. The data are typically rich, abundant and naturally occurring\(^3\). However, they also present some legal and ethical challenges.

Work Package 6 of the SERISS project addresses the major legal and ethical challenges facing cross-national social science research which relies on access to large-scale data at an individual level. The focus is on social surveys and the use of new data types, particularly in a social survey context, including biomarker data, social media data and administrative data. The main focus of Task 6.1 was the legal requirements and ethical challenges that may come about when data arising from electronic communications are obtained from social networks, customer databases and tracking devices. The task addressed the steps that need to be taken to meet these challenges in order to increase and improve the use of these data sources in survey research.\(^4\)

This report is the output of deliverable 6.2 *Guidelines on the use of social media data in survey research*. The main purpose of these guidelines is to provide guidance on the legal requirements and ethical challenges when using social media data in survey research. It is expected that research should safeguard principles of research ethics as well as legal conditions, and in many cases legal conditions overlap with principles of research ethics, as will be discussed further.

These guidelines are structured as Questions and Answers that have been selected with legal and ethical issues in mind. The list of Questions and Answers is not comprehensive, and will focus on a sample of questions that we find most relevant. When using the term ‘legal conditions’ we are referring to the GDPR and other legislation relevant to data processing, whilst ‘principles of research ethics’ are guidelines and standards for good research, which may vary between countries and disciplines.

The guidelines aim to work as advice for researchers and research infrastructures looking to engage in social media data linkage. Note that this is always dependent on the research topic, on which social media data will be collected, and on the methods of analysis that will be used. Note also that these are guidelines rather than rules and that rapid technological advancements will produce new challenges that are not addressed in these guidelines. The questions are structured around the research data lifecycle, covering research design and data collection, data processing, archiving and sharing.

---


\(^2\)http://www.internetlivestats.com/twitter-statistics/

\(^3\)In the ESOMAR Guideline on Social Media Research (2011: 1-2) social media data refers to the information (e.g. photos, comments) that users generate or share while engaged in or with social media. It often includes personally identifiable data.


2 Questions and Answers

Research Design and Data Collection

When do I need to think about the legality and ethics of social media data linkage?
If you intend to link your survey data to social media data sources it is optimal to consider the legal, ethical and technical issues at the very outset of your project. In this way, you may avoid making mistakes that prevent you from conducting the research later on.

Research involving human subjects often requires a research ethics review. Requirements for an ethics review may vary between countries, institutions and disciplines. Large scale studies involving scraping from social media platforms raise the question as to whether the data gathered are to be treated as text (no human input) or as human subjects’ data. In general, the understanding that there has been human input at some point in the process of creation then the consequences for individuals and communities should be considered, even if there is no requirement for a formal research ethics review. If required, ethical approval should be obtained before the study commences (or if the projects changes significantly in the course of the research).

When your research involves processing personal data, which is often the case in projects with linkage to social media data, the data controller must meet certain requirements in the GDPR. Depending on member state law, and the nature of your project, you may be required to have your project assessed by the Data Protection Officer at your institution or an equivalent body. Projects that involve a high risk for social media users (data subjects) will require a Data Protection Impact Assessment (DPIA).

Also, when accessing social media data, permission from the owner/manager of the data (e.g. social media databases) may be required.

What is considered personal data in linked data sets?
The GDPR defines personal data as any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular using an identifier such as a name, an identification number, location data, an online identifier, or using one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (Article 4.1).

In addition to processing names or online identifiers, social media platforms will often include text, videos, audio, quotes and images etc. that can be entered into a search engine and traced back to an individual. Therefore, social media data usually qualifies as personal data.

Survey data in itself may or may not be personal data. This will depend on whether the respondent can be linked to their survey answer, directly via name, IP/-email address etc. or indirectly through background information collected in the survey (such as age, profession, location etc.). However, in order to link survey data to social media data, the respondent must be linked to a unique identifier, for example, their Twitter username. Also, the linking
together of these two types of data can mean that individual persons are more identifiable in the combined data set. For example, a respondent may use an alias as a Twitter username, but the combination of background information collected in the survey and images shared on Twitter can make it easier to identify the respondent.

What information do I need to give to participants?
The GDPR lists the categories of information that must be provided to a data subject in relation to the processing of their personal data, where it is collected from the data subject (Article 13) or obtained from another source (Article 14). For an overview of the required information see the Article 29 Working Party guidelines on transparency, pages 35-40. When administrative data is used as a basis for sampling, both Article 13 and Article 14 apply, and invitation letters and contact sheets must detail the information stipulated in both. The WP29 recommends prioritising communication of the most important information first. This should include:

- the details of the purposes of processing,
- the identity of controller and
- a description of the data subjects' rights regarding their own personal data. These include the right to:
  - access their personal data that being processed
  - request that their personal data is deleted
  - request that incorrect personal data is corrected/rectified
  - receive a copy of their personal data (data portability, when processing is based on consent)
  - object to processing (when the legal basis is public interest)

Further information that will typically be relevant for social media research includes:

- The legal basis for processing,
- categories of personal data concerned,
- recipients of the personal data,
- details of transfers to third countries,
- the storage period for personal data or the criteria used to determine the storage period,
- the right to withdraw consent (when based on consent),
- contact details for the Data Protection Officer
- the right to lodge a complaint with the national supervisory authority
- information about whether personally identifiable data will be published or archived

See appendices A and B for examples on what the information could look like. Please note that this information can also be layered and accessible online.

---

6 http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

www.seriss.eu

GA 654221
Do I always have to give information when linking social media data?
The general rule is that you must inform data subjects about the processing of their personal data in your research project. The obligation to inform is independent of the legal basis for processing personal data.

When you are in direct contact with data subjects, you always have an obligation to provide information. However, in some cases, you may need to collect personal data before you are in direct contact with data subjects. An example of this is when social media data is used to draw a sample for a survey. When you later provide information about the project, this information should explain which personal data you have already collected and why. Exemptions from the obligation to inform are found in Article 14.5 in the GDPR.

Timing of information to data subjects?
The provision of information in a timely manner is a vital element of the transparency obligation and the obligation to process data fairly. When collecting data directly from a data subject the information must be provided “at the time when personal data are obtained”. When collecting from other sources, the required information must be provided within a “reasonable period” after obtaining the personal data and no later than one month. When collecting personal data in order to communicate with potential participants, your obligation to inform is met so long as you give information when you make contact with these individuals.

What is the difference between legal and ethical consent?
It is expected that research should safeguard principles of research ethics as well as legal conditions. In many cases the legal conditions overlap with principles of research ethics. An example of this is consent, which in most cases is a prerequisite for carrying out research where the researcher is in direct contact with participants.

However, ethical consent is not always the same as legal consent. It is a prerequisite for legal consent that you should be able to demonstrate that consent has been gained, and that specific information about participation has been given in advance, i.e. information and consent must be documented/recorded. An ethical consent does not have the same documentation requirement.

Whilst research ethical guidelines may vary between countries, institutions and disciplines, the GDPR sets the framework for a common understanding of the legal conditions for research in countries that have implemented this law. In most cases, complying with the legal conditions will also safeguard principles of research ethics. There are exceptions, but these will not be discussed here.

In some research projects it is not possible to gain legal consent, i.e. consent that meets all requirements for consent in the GDPR. However, if you are in direct contact with data subjects you should always aim to gain ethical consent.
What is granular consent and how could it be applied?

The best way to achieve informed consent for linking and sharing data is to explain to participants what personal data will be processed, how these data will be processed, and for which current and future purposes, and to then offer them the option to consent on a granular level where relevant and possible. The guidelines on Consent from the Article 29 Working Party state that "[…] when data processing is done in pursuit of several purposes, the solution to comply with the conditions for valid consent lies in granularity, i.e. the separation of these purposes and obtaining consent for each purpose." For example, in a qualitative study this may involve allowing the participant to consent to the sharing of anonymized transcripts, non-anonymized audio recordings, and photographs.\(^7\)

If you want to link survey data to social media data, one approach could be to allow participants to choose which data the project is allowed to collect, whilst asking for their consent in the survey. A granular consent could look like this:

<table>
<thead>
<tr>
<th>Please tick the appropriate boxes</th>
<th>yes</th>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>I agree to take part in the survey described in the information letter.</td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>I allow the project to link my social media data to my survey responses [after the survey is finished]</td>
<td>o</td>
<td>o</td>
</tr>
</tbody>
</table>

Depending on the project, one could also imagine a more detailed approach where the respondent is allowed to choose between different social media data to be collected. Like this:

<table>
<thead>
<tr>
<th>Please tick the appropriate boxes</th>
<th>yes</th>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>I agree to take part in the survey described in the information letter.</td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>I agree to allow the project to collect my social media data from blogs and microblogging sites (e.g. Twitter)</td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>I agree to allow the project to collect my social media data from social networking sites (e.g. Facebook)</td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>I agree to allow the project to collect my social media data from content communities (e.g. Instagram)</td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>I agree to allow the project to collect my social media data from collaborative projects (e.g. Wikipedia)</td>
<td>o</td>
<td>o</td>
</tr>
</tbody>
</table>

\(^7\)https://iapp.org/resources/article/wp29-guidelines-on-consent/
\(^8\) Note that this is if consent is the legal basis for processing, not necessarily for ethical consent

www.seriiss.eu GA 654221 7
I agree to allow the project to collect my social media data from virtual game worlds (e.g. World of Warcraft)  

I agree to allow the project to collect my social media data from virtual social worlds (e.g. Second life)  

I allow the project to link my social media data to my survey responses.  

See appendix C for an example of what a consent to link survey data with tweets could look like.  

What is a data management plan?  
A data management plan (DMP) is a document describing how the research data generated in a research project will be handled during the project, and after project completion. The DMP should be prepared at the start of the project in order to help plan and organize the data collection and to become aware of any legal and ethical requirements early in the research process.  

A data management plan will contribute to a legal, structured and safe handling and storing of data. The plan may help you prepare and develop strategies for issues, such as how you plan to obtain informed consent, how data will be stored during the project, how you will control who has access to what data and in what environment, which variables will be linked together, and whether data will be archived after project completion. It can also save time and resources after the project has ended.  

There are a number of sources of guidance for data management planning including the CESSDA Expert Tour Guide on Data Management.  

Data Processing  
When am I processing personal data?  
Article 4 in the GDPR gives us the following definition of processing:  

'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;  

For social media data this means that, for instance, collecting screenshots from Twitter or Facebook with or without an online identifier would constitute processing personal data.  

9 https://nsd.no/arkivering/en/what_is_data_management.html  
11 Funders may require a Data Management Plan.
Whether the data has an online identifier or not, the data can be searched for using a search engine and can be linked back to the user.

What are relevant legal bases for processing social media data?
Processing personal data must be met with one of the legal bases in Article 6.1 in order for it to be lawful. The most relevant legal bases for processing personal data for research purposes are:

- Consent
- A task carried out in the public interest

Consent
Ensuring that research participants have provided «consent» is relevant in determining the legal basis for the processing of personal data. For the consent to be valid (i.e. legal consent), it must be freely given, specific, informed and unambiguous. This means that the person who is asked to participate must be able to understand what participation involves, what they are consenting to, and what consequences participation may have. Be aware that the data controller must be able to demonstrate that informed consent has been gained from the people whose personal data it will be processing (data subjects).

WP29 points out that, according to Article 6 (1), when the researcher is relying on consent as a legal basis, consent must be given for each specific purpose. It goes without saying that specific consent can only be obtained when data subjects are informed about all the intended purposes of data use.

A task carried out in the public interest
Article 6.1 e) in the GDPR gives a lawful basis for the processing of personal data when “processing is necessary for the performance of a task carried out in the public interest”. Here ‘necessary’ means that the processing must be a targeted and proportionate way of achieving your purpose. You do not have a lawful basis for processing if there is another reasonable and less intrusive way of achieving the same result.

It can be difficult to meet the requirements of legal consent when it comes to the requirements for form, content and documentation in the GDPR and the way in which the Article 29 working party have operationalised consent. Also, gaining ‘informed consent’ can be a challenge in complex research projects where it is difficult to ensure that participants understand the implications of their consent (e.g. remember what they have posted, know what they will post, or understand the implications of having their social media data analysed).

This article therefore offers an alternative to processing personal data based on consent. This legal basis can be applicable to projects where ethical consent will be gained, but...
where it will be difficult to achieve research purposes whilst also meeting the documentation requirements for legal consent.

It can also be applicable to complex projects involving linking to social media data where information is provided and ethical consent gained, but where the complexity of the project makes it is difficult to ensure that consent is fully ‘informed’.

As a general rule, the benefit to society of the research being carried out should outweigh the potential impact on the rights and freedoms of data subjects. Note also that this legal basis requires a supplementary national legal basis. You should therefore check to see whether there are special provisions for research in the country where the data controller is based.

In this section we have covered possible legal bases for processing ‘general categories’ of personal data. For processing ‘special categories’ and data relating to criminal convictions and offences you must also have a legal basis in Article 9 and 10 of the GDPR.

Archiving and Sharing

Why deposit research data?

Re-accessing social media data used in prior research may be complicated and expensive or it may be impossible to draw from the same sample or return the same data and metadata in the original structure. Nevertheless, sharing data to the extent, and via the methods, that is/are legal and ethically possible is accepted best practice. Depositing data supports the validation of results, the replication of prior research and the widest possible re-use. Furthermore, archiving data in a trusted digital repository (TDR) helps to ensure the provenance and integrity of the data, ensures long term preservation and maximises the opportunities for citations, which provide credit to the researchers.

Making research data accessible or sharing data for further use is in line with requirements or recommendations from funding agencies and publishers that call for open science. It is also compliant with the FAIR principles (a set of guiding principles to make data Findable, Accessible, Interoperable, and Reusable) for reuse of research data16.

What are the key legal and ethical challenges when preserving social media data?

Some initiatives dealing with ethical issues when preserving social media data already exist and can be used to identify key legal and ethical challenges. At least four areas should be emphasized17:

- Social media platforms’ terms and conditions
- Copyright infringement
- Privacy infringement (consent and anonymity)

17 The following documents have been used to identify these key issues: “Preserving Social Media” (Sara Day Thomson), “Research Ethics and New Forms of Data for Social and Economic Research” (OECD 2016), “Big data and data sharing: Ethical issues” (Libby Bishop), and “Social Media Research: The A Guide to Ethics” (Leanne Townsend & Claire Wallace 2016).
Research integrity

When social media data are linked with survey data, these issues can be further complicated.

Why is it important to consider social media platforms’ terms and conditions?

Even if data are publicly accessible they might not be in the public domain for free use. In most cases, the social media user is not the sole owner of their data, and one of the main legal issues in the use of social media data is the question of data ownership. Social media data is hosted by social media sites, which have different privacy policies, terms of service, and developer agreements\(^\text{18}\) that influence how social media data can be stored and shared.

The various social media platforms (e.g. Facebook, Twitter, Instagram) differ in how they manage their data, and how their users’ data can be used by third parties.\(^\text{19}\)\(^\text{20}\)\(^\text{21}\) In this regard, data archiving is usually complicated. However, data archives may contain data files created from (but not containing) social media data or data links. For example, the current terms of service for Twitter data prevent the sharing of datasets larger than 50,000 Tweets, but do allow for the distribution of tweet IDs and relatively small amounts of derivative data. These may be used by researchers to query the Twitter API and access the raw data.\(^\text{22}\)

It is necessary to study in detail the terms and conditions of social media platforms as some data may be public and usable for research purposes, whilst other data may be of a private nature and hence specially protected. It is also important to note that the terms and conditions of the different social media platforms may change extensively and at short notice, at any point on the research data lifecycle (sometimes the changes may even reflect changes in legislation, such as when the GDPR came into force).\(^\text{23}\)

What about copyright infringement?

Another issue that should be emphasized in the case of social media data is the risk of copyright infringement. Aggregation of social media data is dependent on text and data mining of individual contributions from large databases that may be protected as copyrighted works. Copyright issues can be relevant for example when it comes to qualitative analyses where authors may want to reproduce social media content in publications. With regard to archiving and preserving data from social media, Day Thomson notes that\(^\text{24}\):

\[\text{18} \text{Day Thomson 2016}\]
\[\text{19} \text{For Facebook Data Policy, see: Facebook full data use policy}\]
\[\text{20} \text{For Twitter see Terms of Service and https://help.twitter.com/en/rules-and-policies/twitter-api}\]
\[\text{21} \text{For Instagram see: Terms of Use}\]
\[\text{22} \text{Twitter make special provisions regarding sharing tweet IDs for academics conducting non-commercial research (Sloan, Jessop, Al Baghal, Williams “Linking Survey and Twitter Data: Informed Consent, Disclosure, Security and Archiving”, draft 28/03/19).}\]
\[\text{23} \text{For the data archives or repositories, one possibility could be to have an agreement with the data producer or owner. This is also suggested by Weller and Kinder-Kurlanda (2016) who suggest establishing dialogue between social media companies, researchers, and data repositories to “establish feasible interpretations of terms of service that allow researchers to at least share data for the sake of quality control and reproducibility” (Hull and Mannheimer 2017: 203).}\]
\[\text{24} \text{Day Thomson 2016: 17}\]
the infringement of copyright in the instance of researchers using individual pieces of copyright-protected content, such as images or sound, does not become an issue unless the researcher wants to publish or otherwise distribute a copy of the image contained in the data. If researchers publish analysis of large aggregates of user data (as opposed to individual user accounts or posts), there is less (or no) risk of copyright infringement. Therefore archiving and preserving large aggregates of user data from social media APIs poses very little risk of infringing copyright.

For data archives, copyright challenges encompass both the issues of copyright in deposited materials and the need to manage any collaborative platforms that support the uploading of content by researchers.\(^{25}\)

Has consent been obtained?
It has been noted that platform-specific usage norms can affect a user's expectation of privacy, and that “[t]he most unambiguous method for aligning research with user expectations is to obtain informed consent”.\(^{26}\) When your research involves active participation by social media users then you are in a position to explain the current and future uses of the collected data (so that users know what to expect) and can gain informed consent for data archiving during data collection. Gaining consent is arguably best practice when you are in contact with data subjects, both when it comes to ethical considerations and enabling lawful archiving pursuant to the GDPR.

However, in cases where archiving was not planned in advance, or where the consent that has been gained is not sufficient (e.g. not specific enough), there is an alternative legal basis that may be applicable. Personal data may be processed for a task in the public interest, more specifically “for archiving purposes in the public interest”.\(^{27}\) When archiving personal data with this legal basis, appropriate safeguards must be in place and the archiving purposes should not be incompatible with the initial purposes.\(^{28}\)

Data curators should check whether consent has been obtained before archiving social media data. If consent does not meet the requirements of legal consent, then another legal basis for archiving may be applicable. Note that the data controller must document the legal basis for processing personal data, also for archiving purposes.

When is social media data anonymous?
The GDPR does not apply to data that “does not relate to an identified or identifiable natural person (anonymous information) or to data rendered anonymous in such a way that the data subject is no longer identifiable.” The GDPR also distinguishes between anonymization and

\(^{25}\) L'Hours et al 2018: 8
\(^{26}\) Mannheimer and Hull 2017: 201
\(^{27}\) Legal basis in article 6 (1)(e) with archiving as a specific processing situation, as provided for in Article 89
\(^{28}\) See Article 5 (1) (b) and Article 89 (1) and (3) in the GDPR. Note that this legal basis allows for specific provisions and derogations in Member State law.
pseudonymisation of data. Pseudonymised data means personal data that can no longer be attributed to a specific data subject without the use of additional information that is kept separate (i.e. a scrambling key). Data that are not completely anonymized but merely pseudonymized are still considered to be “personal data”. For any personal data, the legal and ethical issues must be addressed between the depositor and the data archive or repository:

(M)aking data available through a repository may be more democratic, but careful consideration must be given to whether repository conditions match confidentiality commitments given to data subjects and possible risks from data linkage.\textsuperscript{29}

Since social media companies may store data and metadata for long periods, and much of this data is searchable, anonymization for secondary use of data is challenging. For example, even if the author field is removed it would be possible to search for content online.\textsuperscript{30} Nevertheless, in cases of “aggregate data where individual units or postings are no longer discernible, it is generally safe to share the data set”\textsuperscript{31}.

Anonymization is further complicated when survey data is linked to individuals’ social media data. Al Baghal et al\textsuperscript{32} note that if directly linked to survey responses, Twitter data could deanonymize the survey responses and any identifying information such as Twitter handles and tweet text would need to be stripped to make the linked data anonymous. However, Twitter’s terms and conditions are explicit in that individual data extracts such as Tweets should not be amended. The process of anonymising data could also reduce the value of the data for secondary analysis. In such circumstances, in particular if survey data is linked to social media data of individuals, secure access systems may be utilised.

In order to protect users it is recommended that you consider a wider range of factors, including the specific context, the research topic and the user-group.

Can direct quotes be published as part of a research paper/report?

Be aware that direct quotes might be searchable on the Internet. Pseudonyms or nicknames may also be identifiable because they might be used in various online contexts and can hence function as a digital identity.\textsuperscript{33} Since quotes, metadata, and online identifiers could all be used to identify individuals, the researcher is advised to treat social media data as personal data.

ESOMAR recommends “masking” for cases where there is no consent to publication. Masking is “a technique whereby the original social media data such as comments, photos or videos is altered to a point that it cannot be traced back or attributed to the original user

\textsuperscript{29}Weller & Kinder-Kurlanda, “Uncovering the Challenges in Collection, Sharing and Documentation: the Hidden Data of Social Media Research?”
\textsuperscript{30}Evans, Ginnis Bartlett, “A guide to embedding ethics in social media research”, (2015: 4)
\textsuperscript{31}Townsend & Wallace 2016: 13
\textsuperscript{32}2019: 11-12
\textsuperscript{33}Segadal in Fossheim and Ingjerd, “Internet Research Ethics”, 2015: 43.

www.seriss.eu GA 654221
(using a search engine for example)^34. Nonetheless, this approach conflicts with Twitter’s current policy which states “Do not modify, translate or delete a portion of the Content”^35. On an individual level one could also ask for consent to publish personal data from social media.

What about research integrity?

To ensure transparency and replicability, data should have a clear provenance. Also, the sources and processing of the data sets made available for others should be known, identified, and documented.36 Social media data are mostly not archived in a form which would secure full transparency and replicability. Compared to traditional data files, where a copy of the original data set can be deposited within a data archive and the changes made to the data set can be documented, social media data (e.g. original data available through platform API) is neither static nor guaranteed to be available over time. For example, the identical recreation of a dataset is only possible if no tweets are deleted after the original dataset is created. Social media platforms’ terms and conditions may also change, presenting another challenge to maintaining compliance when data has been deposited within an archive.37

Is there any infrastructure for archiving social media data?

There is currently no exclusive infrastructure for archiving social media data. In most cases, web archives do not cover social media in their harvests (or only in a limited way).38 While social media platforms themselves may store data, the availability of this data for academic research is limited.

The evolving technical infrastructures that provide data depositing/storage/discovery services may ensure bit-level integrity but will not always offer curation and preservation independently of the data depositor. These include Figshare and Zenodo, which “makes no promises of usability and understandability of deposited objects over time”^39^40. Domain and disciplinary repositories will undertake to curate and preserve research data for the long term and often support more advanced metadata to support the discovery and understandability of the data. For the social sciences these include the CESSDA archives^41. Some of these are classified as Trustworthy Digital Repositories (TDR) which are accredited to standards (e.g. CoreTrust Seal^42) which provide assurances that, in addition to ensuring bit-level assured storage, the data will be preserved for the long-term. The registry at re3data^43

---

34 ESOMAR Guideline on Social Media Research 2011
36 Bishop 2017: 5
37 L’Hours et al 2018b: 23. See also SERISS D6.8 “Versioning requirements for curation and access to new forms of data” and D6.9 “Appraisal/Selection Requirements for New Forms of Data”.
38 Note that this is an area which is rapidly developing and some repositories are currently developing methods to archive and collect social media data such as CLARIN repositories (e.g. CLARIN SI project). The Social Media Archive (SOMAR) at ICPSR and the Australian project TriSMA – Tracking Infrastructure for Social Media Analysis are other examples.
39 https://knowledge.figshare.com/articles/item/preservation-and-continuity-of-access-policy
40 http://about.zenodo.org/policies/
41 https://www.cessda.eu/About/Consortium/Membership
42 https://www.coretrustseal.org/about/
43 https://www.re3data.org/
provides a registry of research data repositories. Institutions or funders may also provide specific requirements or guidance on which archives or repository types to use.

How can social media data be deposited within a data archive?

Whether social media data can be deposited within a data archive or not is dependent on the kind of data that have been collected, the platform in use, as well as technical, legal and ethical issues. Although various research projects are currently using social media data, there are few datasets available for secondary analysis and replication. Still, some possible solutions can be assessed through looking at studies that have already been carried out.

The following tables include examples of data sets that have been successfully archived at UK Data Archive and GESIS. Both of the examples include data that was collected using the Twitter API. Note that these are not linked data sets.

<table>
<thead>
<tr>
<th>Cram, Laura and Llewellyn, Clare (2017) UK-EU referendum Twitter data. [Data Collection]. Colchester, Essex: UK Data Archive. 10.5255/UKDA-SN-852513</th>
</tr>
</thead>
<tbody>
<tr>
<td>This data collection consists of Tweet IDs collected on the UK-EU referendum between September 2015 and August 2016.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Kaczmirek, Lars; Mayr, Philipp (2015): German Bundestag Elections 2013: Twitter usage by electoral candidates. GESIS Data Archive, Cologne. ZA5973 Data file Version 1.0.0, doi:10.4232/1.12319</th>
</tr>
</thead>
<tbody>
<tr>
<td>The data includes the Tweet-ID and an ID identifying the candidates. The list can be used to retrieve the original tweets, which were posted between June and December 2013.</td>
</tr>
</tbody>
</table>

The following table includes an example of data archived at GESIS. The data set contains information on parties’ Facebook posts during the six weeks of election campaign for the Austrian general election in 2013.

<table>
<thead>
<tr>
<th>Müller, Wolfgang C.; Bodlos, Anita; Dolezal, Martin; Eder, Nikolaus; Ennser-Jedenastik, Laurenz; Kaltenegger, Matthias; Meyer, Thomas M.; Praprotnik, Katrin; Winkler, Anna Katharina (2017): AUTNES Content Analysis of Party Facebook Pages 2013. GESIS Data Archive, Cologne. ZA6882 Data file Version 1.0.0, doi:10.4232/1.12699</th>
</tr>
</thead>
</table>

How can I prepare my data for archiving and sharing?

Firstly, you have to make sure that the data can be shared in accordance with legal and ethical frameworks. If personal data is to be archived the legal relationship with the data owner must be clear, and depositors should provide documentation to confirm this.

Further, when depositing data within a data depository, data should be clearly documented to make sure that the data can be understood, also in the future. Both information about the data itself and the study for which the data has been collected should be provided, such as study title, data type, the sponsor of the research and criteria for selection. In cases where

---

44 One example of a study where a panel was asked for consent to link Twitter data is the British Social Attitudes (BSA) survey 2015. As part of an interview respondents were asked whether they had a personal Twitter account, and if the respondent said they had an account they were further asked whether they would consent to link their Twitter data to their survey responses. If the respondent consented, they were then asked to provide their Twitter username (Al Baghal et al 2019: 5-6).
social media data have been linked to survey data, documentation could also include explanations about the source of the data, the specific process by which it was collected, which variables that have been linked together etc. Detailed documentation of the research procedures (e.g. scripts, list of accounts) can allow others to check how the collection of data, cleaning and analysis have been performed.4546

Due to the novelty of social media data, standards and methods are not firmly established across disciplines.47 Recommendations on how to document and format your data can be found in data repositories that usually follow a metadata standard48. There are also other resources available to assist researchers in documentation such as CESSDA’s training suite49.

46 L’Hours et al (2018: 17) notes that additional documentation and metadata can be required when, for instance, linked data have different levels of provenance or perceived technical data quality (e.g. survey data vs. social media data).
47 Day Thomson, “Preserving Social Media”, 2016: 13
49 https://www.cessda.eu/Training/
## Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Abbr.</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anonymous data</td>
<td></td>
<td>Data that cannot be linked to individuals in the data set; not directly e.g. name, online identifier or social security number, indirectly through background variables, nor through a list of names/usernames or an encryption formula and code/scrambling key.(^{50})</td>
</tr>
<tr>
<td>Consent</td>
<td></td>
<td>Consent from data subjects (i.e. legal consent according to the GDPR) is any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of personal data relating to themself.(^{51})</td>
</tr>
<tr>
<td>Data access</td>
<td></td>
<td>The activity by which a researcher is given access to data.(^{52})</td>
</tr>
<tr>
<td>Data controller</td>
<td></td>
<td>'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.(^{53})</td>
</tr>
<tr>
<td>Data curation</td>
<td></td>
<td>The activity of managing and promoting the use of data from its point of creation, to ensure it is fit for contemporary purpose, and available for discovery and re-use. A more formal definition is: Digital curation is all about maintaining and adding value to a trusted body of digital information for future and current use: specifically, the active management and appraisal of data over the entire life cycle.(^{54})</td>
</tr>
<tr>
<td>Direct identifier</td>
<td></td>
<td>A person will be directly identifiable through name, social security number or other unique, personal characteristics.</td>
</tr>
<tr>
<td>Data management plan</td>
<td>DMP</td>
<td>A DMP is a formal document that provides a framework for how to handle the data material during and after the research project.(^{55})</td>
</tr>
<tr>
<td>Data processor</td>
<td></td>
<td>Processor means a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller.(^{56})</td>
</tr>
</tbody>
</table>


\(^{51}\) GDPR Article 4

\(^{52}\) OECD 2016: 41

\(^{53}\) GDPR Article 4

\(^{54}\) OECD 2016: 41


\(^{56}\) GDPR Article 4
| FAIR principles | FAIR | A set of guiding principles to make data Findable, Accessible, Interoperable, and Reusable.  
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>General Data Protection Regulation</td>
<td>GDPR</td>
<td>The GDPR (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the European Council and the European Commission intend to strengthen and unify data protection for individuals within the European Union (EU). It came into force in May 2018.</td>
</tr>
</tbody>
</table>
| Indirect identifiers | | A person will be indirectly identifiable if it is possible to recognize the person through background information such as place of residence or institutional affiliation, combined with data on age, gender, occupation, diagnosis, etc.  
| Long-term preservation | | In data management, data preservation is the process of maintaining access to data so that it can still be found, understood and used in the future.  
| Metadata | | Provides information on data and the processes of producing and using data. Metadata are data which are needed for proper reproduction and use of the data  
| Open access | | Open access can be defined as the practice of providing online access to scientific information that is free of charge to the reader. In the context of research and development, open access typically focuses on access to 'scientific information' or 'research results'.  
| Personal data | | Any information relating to an identified or identifiable person. A person may be identified by e.g. name/username, online identifier, email, IP address or a number referring to a list of names, through photo/video of recognizable faces, or through a combination of background information.  
| Research data | | May be defined as information relevant to, or of interest to, researchers either as inputs into or outputs from research. They are research materials resulting from primary data collection or generation, or derived from existing sources intended to be analysed in the research project.  
| Synergies for Europe's Research Infrastructures in the Social Sciences | SERISS | A Horizon 2020 project focused around three key themes – key challenges facing cross-national data collection, breaking down barriers between research infrastructures, and embracing the future of social sciences. It addresses issues  

---

57 https://www.force11.org/group/fairgroup/fairprinciples  
59 https://www2.le.ac.uk/services/research-data/keep-data/lterm-pres  
60 OECD 2016: 42  
61 http://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-dissemination_en.htm  
63 OECD 2016: 43
relating to survey design and data collection, data management and curation from a collaborative, cross-national perspective. The project will better equip Europe’s social science data infrastructures to play a major role in addressing the key societal challenges facing Europe today and help ensure that national and European policymaking is built on a solid base of socio-economic evidence that is of the highest-quality. See [www.seriss.eu](http://www.seriss.eu).

| Social media | Internet based platforms and technologies that permit users’ interaction and/or facilitate the creation and exchange of user generated content. Examples include online forums, social networks (e.g. Facebook), video/photo sharing (e.g. YouTube).64 |
| Social media data | Social media data refers to the information (photos, comments, etc.) that users generate or share while engaged in or with social media. It often includes personally identifiable data.65 |
| Social media research | Social media research encompasses all research where social media data, the information that users generate or share within social media platforms, is used for research purposes either by itself or together with information from other sources. Examples include monitoring or crawling social media platforms and ethnographic research like observing online social behaviour.66 |
| Trusted digital repository | TDR A trusted digital repository is one whose mission is to provide reliable, long-term access to managed digital resources to its designated community, now and in the future.67 |

64 ESOMAR Guideline on Social Media Research (2011: 1-2)
65 ESOMAR Guideline on Social Media Research (2011: 1-2)
66 ESOMAR Guideline on Social Media Research (2011: 2)
67 [https://www.oclc.org/research/activities/trustedrep.html](https://www.oclc.org/research/activities/trustedrep.html)
Appendix A: Example Information Letter

This first example is made by NSD – Norwegian Centre for Research Data and their section for data protection services for research. This is a template for informed consent when processing personal data in a research project where survey data will be linked to social media data (consent as lawful basis consent). Please delete the text in *italics* and insert text that fits your project. NB: Please note that this information can also be layered and accessible online. You may wish to gain explicit consent for linking after the respondent has filled out the survey.

**Are you interested in taking part in the research project**

"*[insert title of project]*"?

**Purpose of the project**

We invite you to participate in a research project that aims to *[insert description of the project purpose, objectives/research questions]*.

*Indicate the scope of the project and whether it is a research project, a doctoral thesis etc.*

*If you or others will use the collected personal data for other purposes (e.g. teaching or other research projects), describe these other purposes.*

**Who is responsible for the research project?**

*[Insert name of the institution(s)]* is the institution responsible for the project.

*If applicable, provide names and describe cooperation with other institutions, external entities etc.*

**Why are you being asked to participate?**

*Describe how the sample has been selected (population, selection criteria (including lower age limit) and how many people have been asked to participate), so that it is clear why the person is receiving this invitation.*

*If applicable, indicate whether you have received the person’s contact details from another (and indicate any approval/permission obtained in order to do this), or whether another has sent out this information letter on your behalf.*

**What does participation involve for you?**

*Describe the methods (e.g. online survey and linking to social media data), what type of data will be collected and how the information will be recorded (electronically) e.g.:

« If you choose to take part in the project, this will involve that you fill in an online survey. It will take approx. 30 minutes. The survey includes questions about (describe the most important questions/topics). Your answers will be recorded electronically. If you give consent, we will link your survey answers to publicly available information from your (Facebook/Twitter) account such as (profile*
Participation is voluntary
If you choose to participate, you can withdraw your consent at any time without giving a reason. All information about you will then be made anonymous. There will be no negative consequences for you if you choose not to participate or later decide to withdraw consent.

Your personal privacy – how we will store and use your personal data
We will only use your personal data for the purpose(s) specified in this information letter. We will process your personal data in a confidential manner and in accordance with data protection legislation (the GDPR).

- Describe which persons, internal to the data controller, will have access to the personal data (e.g. the project leader, the project group etc.)

- Indicate the name of any data processor (i.e. online survey provider) that will be used to carry out the survey and will process personal data on behalf of the data controller

- Describe which measures you will take to ensure that no unauthorized persons are able to access the personal data, e.g. «We will replace your name/username with a code. The list of names/usernames (or other online identifiers) and respective codes will be stored separately from the rest of the collected data», that you will store the data on a secure research server, encrypted, etc.

If applicable, indicate:

- that persons from other institutions will be given access to the collected personal data, name the institutions and explain what type of information they will have access to (e.g. whether they will have access to data that can be linked directly to individual participants, or to pseudonymised data etc.)

- that personal data will be processed outside the EU (e.g. cloud computing, conferences), name the institution and country, describe security measures.

Describe whether participants will be recognizable in publications or not, and to what extent. If applicable, indicate what type of personal information will be published (e.g. username, background information, direct quotations from social media data etc.).

What will happen to your personal data at the end of the research project?
The project is scheduled to end by approximately [MM/YYYY]. Describe what will happen to the personal data at the end of the project (e.g. storage for a set period of time, archiving, anonymisation, deletion etc.).

If the collected data will not be anonymised at the end of the project: indicate the purpose of further storage/use of personal data (e.g. verification, follow-up studies, archiving for
future research), indicate where the personal data will be stored, who will have access to it, and the date for anonymisation/deletion (or, if applicable, specify that the personal data will be stored indefinitely and give a reason for this).

Your rights
So long as you can be identified in the collected data, you have the right to request access to your personal data, request that your personal data is corrected or deleted, and request a copy of your personal data. You also have the right to lodge a complaint with your national supervisory authority regarding the processing of your personal data.

What gives us the right to process your personal data?
We will process your personal data based on your consent.

Where can I find out more?
If you have questions about the project, or want to exercise your rights, contact:
- [Insert name of data controller] via [insert name of the project leader and contact details]
- Our Data Protection Officer: [insert name of the data protection officer and contact details]

Consent
I have read the above information about the project [insert project title] and understand that I can contact the project to ask questions and exercise my rights. I give consent:

- □ to participate in this online survey
- □ for my survey answers to be linked to my data that I have shared on social media (e.g. Twitter/Facebook) under the username/handle ______________________
- □ for my personal data to be processed until the end of the project, approx. [MM/YYYY]
- □ for my personal data to be stored after the end of the project until approx. [MM/YYYY] for [insert purpose of storage e.g. follow-up studies, validation]
- □ for my survey data and my data that I have shared on social media to be published in research publications in a way that I can be recognised
Appendix B: Example Information Letter

The second example is from the European Social Survey. This information sheet was not meant to be a template and the national teams are encouraged to adapt the information. The letter contains the information one needs to provide the data subjects in order to comply with the information requirements in the GDPR.

The European Social Survey is a survey of social attitudes, beliefs and behaviours of individuals in European countries

Protecting your personal information is important to us. This leaflet outlines what we do with the information we collect and store.

Why are we contacting you?
[ESS has asked National statistics agencies to produce representative lists of possible participants, based on random sampling information about [your age, gender, address] or household].

If you are under 16 years of age at the time of the interview, a parent or guardian will be asked for permission for you to participate. As a parent/guardian you can request to see the questionnaire in advance.

Your participation in the ESS
During the ESS interview, you will be asked a number of questions about your attitudes, life events, as well as more factual questions. We will ask about, politics, religion, trade union membership and about your attitudes to social issues. Your answers from the interview will be recorded electronically. We also gather information about the area you live in.

Your participation in the survey is voluntary. You are free to choose which questions you want to answer, and you may stop the interview at any time without giving any explanation.

If you decide not to participate
If you decide not to take part in the ESS, for whatever reason, we will ask and record the reason(s) why, for example if this is due to a language barrier or illness/sickness. This information helps us to check that the people who participate in the survey are representative of the overall population in your country. For information about your privacy and rights, see below.

What happens with the collected information?
❖ We will treat all the information about you with strict confidentiality and in accordance with EU’s General Data Protection Regulation (GDPR) and national data protection laws.
❖ Only the [FWO], that collects data, will have access to your contact (eg name and address) information.
❖ When the survey is finished, the [FWO] will send the ESS-data, without your name or contact details to the ESS Archive (NSD - Norwegian Centre for Research Data, Bergen, Norway).
❖ Your name and contact information will be deleted when the data is published and no later than June 2020.
❖ The rest of the collected ESS-data will be securely stored for an indefinite period. They are made available for use in scientific studies by researchers, students and others interested in Europeans’ social attitudes.
❖ There is a possibility but it is unlikely that some information (such as citizenship, age, country of birth, occupation, ancestry and region may combine in a way that would identify you. This is a possibility only for the survey responses which are not published. Access to these data will only be given to researchers after approved applications and confidentiality agreements are in place.
❖ The results of the survey will be published on the ESS website within May 2020.
❖ We will make every effort to ensure that no participant is identifiable in the results of the survey or in any publications based on the study.

Your rights
As long as we can identify you in the ESS results (the survey responses), you have the right to object to the processing of your personal data, to access, rectify and erase any information about you, and to ask us what information we hold about you. Once details such as your name and address are removed, then it will no longer be possible to delete the information you provided.

You also have the right to lodge a complaint to your national supervisory authority or with the UK Information Commission’s Office.

Who is responsible?
The European Social Survey European Research Infrastructure Consortium (ESS ERIC) undertakes the survey and is the Data Controller. Its headquarters are in London, UK.

What organisations are involved?
In [country], [Name of National Coordinator] at [Institution] and [the fieldwork agency] is responsible for the recruitment and carrying out the survey. See [link to national websites] for an overview of the key members of this team.

What gives us the right to collect your personal data?
The lawful bases used in ESS are that it is undertaken as a task in the public interest and necessary for research and archiving purposes, in accordance with the General Data Protection Regulation and national laws.

Where can I find out more?
To find out more about the study, visit [national ESS web page] and www.europeansocialsurvey.org

www.seriss.eu GA 654221
Contacts:
FWO/National team [enter phone number] [email]

Data Protection Officer, ESS ERIC (Data Controller):
dpo.esseric@europeansocialsurvey.org

National Data Protection Authority: [enter contact details]

UK Information Commission’s Office
By Post: Wycliffe House
Water Lane
Wilmslow Cheshire
SK9 5AF
By Telephone 01625 545700
https://ico.org.uk/global/contact-us/email/

Full privacy notice at: www.europeansocialsurvey.org/about/privacy.html
Appendix C: Example Twitter Consent Module

---

For further information see: https://www.understandingsociety.ac.uk/documentation/innovation-panel/dataset-documentation/wave/10/questionnaire-module/twitterconsent_ip10

---

For further information see: www.seriss.eu  GA 654221
References


Bishop, L (2017) Big data and data sharing: Ethical issues. UK Data Service, UK Data Archive.


CoreTrustSeal (2018) Retrieved from https://www.coretrustseal.org/about/


Digital Preservation Coalition 2016 and Sara Day Thomson (2016) Preserving Social Media. DOI: http://dx.doi.org/10.7207/twr16-01


Kaczmirek, L & Mayr, P (2015) German Bundestag Elections 2013: Twitter usage by electoral candidates. GESIS Data Archive, Cologne. ZA5973 Data file Version 1.0.0. DOI:10.4232/1.12319


L’Hours, H et al (2018b) Versioning Requirements for Curation and Access to New Forms of Data. Deliverable 6.8 of the SERISS project funded under the European Union’s Horizon 2020 research and innovation programme GA No: 654221. https://doi.org/10.5281/zenodo.1406217


www.seriss.eu

GA 654221


