SIGN HUB

European Commission | Horizon 2020 European Union funding for Research & Innovation

Project Number: 693349

D1.5 OUTLINE OF DATA MANEGEMENT PLAN

Authors

Josep Quer
Marco Indaco
Jordina Sánchez Amat

Version 1.3 – 29/09/2016

Lead contractor: Universitat Pompeu Fabra

Contact person:

Josep Quer
Departament de Traducció i Ciències del Llenguatge
Roc Boronat, 138
08018 Barcelona
Spain

Tel. +34-93-542-11-36
Fax. +34-93-542-16-17

E-mail: josep.quer@upf.edu

Work package: WP1

Affected tasks:

Nature of deliverable[1]	R	P	D	O
Dissemination level[2]	PU	PP	RE	CO

[1] *R: Report, P: Prototype, D: Demonstrator, O: Other*

[2] ***PU**: public, **PP:** Restricted to other programme participants (including the commission services), **RE** Restricted to a group specified by the consortium (including the Commission services), **CO** Confidential, only for members of the consortium (Including the Commission services)*

COPYRIGHT

CONTENTS

Scope of the document

This document presents the first outline of the Data Management Plan of the SIGN-HUB project. It addresses all the aspects required to the extent that they have been tackled and planned at this stage of the project (month 6).

1. Data summary

1.1. Purpose of the data collection/generation in relation to the objectives of the project

The fieldwork is carried out mostly in work package 2 (WP2 CONTENT), which is formed by the tasks and objectives listed below (SIGN-HUB Grant Agreement, Description of the Action, p. 14):

- Task 2.1. The first objective is to implement the SignGram Blueprint (outcome of COST Action IS1006) to produce online grammars of the following European sign languages: German Sign Language (DGS), Catalan Sign Language (LSC), Spanish Sign Language (LSE), Italian Sign Language (LIS), Sign Language of the Netherlands (NGT) and Turkish Sign Language (TİD).
- Task 2.2. The second objective is to produce an interactive online atlas of the sign languages of the world. This will be hosted in a technologically high standard platform for that will provide grammatical and socio-linguistic information of European and non-European sign languages.
- Task 2.3. The third objective is to develop reliable tests to assess sign language impairments in signing populations that are able to distinguish between poor performance due to late language learning and poor performance as a result of a language disorder. We will design assessment tools for the following sign languages: LIS, LSF, ISL, LSC and LSE, and develop general guidelines for the development of similar tools in other sign languages.
- Task 2.4. The fourth objective is to create a digital archive of old signers' linguistic and cultural heritage. We will systematically record, document, analyze, and make available online the linguistic uses as well as the cultural heritage and historical memories of elderly deaf people in Germany, Italy, the Netherlands, Spain, and Turkey, while in France and Israel SIGN-HUB we will digitalize and/or extend existing archives of deaf signers that are at the risk of loss.

Tasks 2.1 and 2.2: Creation of online grammars and atlas of sign languages

In order to implement this task, data on linguistic abilities will be collected from native or highly fluent near-native signers. Participants will be asked either to produce a sentence in their language after attending to an explanation, seeing a photo, a drawing or a video about an object or an action; or to watch a sentence in sign language and to evaluate it grammatically, or to tell a story or a narrative in their language.

The data will be collected through video recordings. They may also be asked to fill out a questionnaire which will help the researchers to find out their linguistic background such as information on the language use of the parents, the timing of exposure to sign language, amount of sign language used during their education, and the variety of sign language used (i.e. dialectal information). This information will become the metadata of the linguistic material gathered in the elicitation sessions.

Task 2.3: Development of tools for sign language assessment:

In order to implement this task, sign linguistic data will be collected from three different groups of participants in 4 countries (Italy, France, Israel and Spain). Participants will be recruited in connection with the length of their sign language experience and education: native

signers; early learners, having been exposed to sign language before the age of 7, and late learners, having been exposed to sign language between age 8 and 13.

Participants will be asked to undertake different tasks in order to evaluate their comprehension of single signs and sentences, their production of single signs and their phonological and syntactic abilities. The data will be collected through video recordings.

Task 2.4: Digital Archive of old signers' linguistic and cultural heritage

To this end, data from elderly signers (age 70 and older) from Germany, Italy, the Netherlands, Spain and Turkey will be collected (in France and Israel the digital archive will include existing film materials, see section §1.3). Data will be collected by means of video-recordings from elderly Deaf signers in close interaction with the local Deaf communities.

The interview will be semi-structured and the same main set of questions will be used in all countries, although each national unit will add specific topics related to the situation of the local Deaf community.

Representative samples of the interviews will be subtitled in the local spoken and/or English in order to set the ground for the preparation of a documentary film about signers' linguistic and cultural heritage.

Tasks 3.1-3.6: Developing the digital infrastructures to host the contents produced by the other tasks and to disseminate samples of them

Surveys or focus groups will be used in the development of the digital infrastructures and to test its services functionalities and interfaces. Different groups of signers at national level will be recruited to these ends.

1.2. Types and formats of data generated/collected

The data will be mainly collected through video recordings, but written questionnaires and surveys will be also used to collect background data about participants and to produce online grammars (see Table 1).

Table 1. Type and format of data generated/collected related to the aim to which it contributes.

Task	Video recording	Questionnaires / surveys	Format	Aim
2.1	x		MP4, AVI	To implement the SignGram Blueprint to produce online grammars.
		x	xls	Metadata: to find out the participants' linguistic background such as information on the language use of the parents, the timing of exposure to sign language, amount of sign language used during their education, and the variety of sign language used.
2.2	x		MP4, AVI	To illustrate linguistic features.
		x	xls	To illustrate linguistic features.
2.3	x		MP4, AVI	To develop tools for sign language assessment.
		x	xls	Metadata: to find out the participants' linguistic background such as information on the lan-

Task	Video recording	Questionnaires / surveys	Format	Aim
				guage use of the parents, the timing of exposure to sign language, amount of sign language used during their education, and the variety of sign language used.
2.4	x		MP4, AVI	To build a Digital Archive of old signers' linguistic and cultural heritage
3.1-3.6		x	xls	To develop the digital infrastructures and to test its services functionalities and interfaces

1.3. Existing data re-use

In order to achieve the SIGN-HUB goals, some existing data will be re-used.

As for Task 2.4, in France and Israel the digital archive will include existing film materials (narratives of and interviews with Deaf subjects). In order to use these preexisting materials and to disseminate them openly through the internet, the appropriate permissions (such intellectual property rights) will be obtained.

Regarding the French Deaf community, there are several Deaf associations that have video archives of VHS and other magnetic supports which document how Deaf people lived during War World II, the Algerian War, and demonstrations to support Deaf people rights, for instance. These recordings include post-event semi-structured interviews and in some cases even live recordings of the events. These materials are often very badly shielded, and preservation of magnetic supports is an unsuitable solution that would condemn the content of the videos to an unavoidable loss. As part of task 2.4, CNRS and CINI will digitize part of the archive of the Académie de la Langue des Signes Française (http:// www.languedessignes.fr/).

As for Israel, TAU will catalogue, digitalize (when necessary) and organize for future linguistic research existing videos in sign language of Deaf Holocaust survivors and of their families. This will be done with the cooperation of the Institute for the Advancement of Deaf Persons in Israel and the Association of the Deaf in Israel. Existing interviews with elderly Israeli Deaf individuals collected at the Sign Language Laboratory of the University of Haifa are also likely to be incorporated.

1.4. Expected size of the data

Sign language videos will represent the majority of the contents produced by the project in terms of bites. Current video technology achieved excellent results in terms of high definition and digital technology. Still, some issues are open, especially those concerning the balance between quality of the digital image and the size of video files, streaming of contents on mobile devices and availability of bandwidth.

The expected total size of the videos recorded surpasses 400 GB (see Table 2).

Table 2. Calculation of the expected size of the data.

Task	Estimated time recorded/video	Estimated size/video	Participants/SL	Number of sign languages	Total size
2.1	30 min	500 MB	Not specified (2 at least)	7	7 GB

Task	Estimated time recorded/video	Estimated size/video	Participants/SL	Number of sign languages	Total size
2.2	Extracted from videos collected in task 2.1	Extracted from videos collected in task 2.1	Not specified	7	?
	15 min	250 MB	Not specified yet	Not specified yet	?
2.3 (phase 2)	30 min	500 MB	45	5	113 GB
2.3 (phase 3)	30 min	500 MB	Not specified yet	2	?
2.4	1 h	1 GB	20-30	6 (+2; existing files)	240 GB
2.4	3 h	3 GB	20-30	6	540 GB
					Total: >940 GB

1.5. Data utility

Access to the SIGN-HUB project data will be useful for the following stakeholders: research community, policy makers and Deaf citizens.

Research community and scientific activity

SIGN-HUB has been designed to generate comparative, in depth and scientifically grounded knowledge about the grammar of sign languages, their typological, synchronic and diachronic variation, and their acquisition. Data provided by SIGN-HUB will allow and enhance research in the following fields, among others (SIGN-HUB Grant Agreement, Description of the Action, p. 16-17):

- Sign languages grammar descriptions
- Typological and comparative research into the signed modality
- Cognitive processes associated with language acquisition in exceptional circumstances and in bimodal bilingualism
- Factors at play in language change by adding sign languages to the field of historical linguistics
- The recent history of European minorities

Policy makers

The availability of accurate grammatical descriptions will have a direct impact in the following areas (SIGN-HUB Grant Agreement, Description of the Action, p. 17-18):

- In education, where a reliable linguistic basis is required for the development of sign language curricula and teaching materials for Deaf children, who will be taught in sign language and about sign language. At the same time, it will improve the proficiency of all professionals involved in the schooling environment, such as teachers, language therapists and interpreters;

- In interpreter training, which unlike the spoken language interpreter education, lacks a proper background linguistic knowledge, and more generally in teaching of sign language as a second language;
- For the quality control of interpreting services, which are so critical for Deaf citizens when interacting with the hearing environment (health care, justice, administration, etc.);
- In language assessment in educational and clinical contexts, which are deprived of proper tools to evaluate language development (for instance, in placing incoming children in the most adequate class in school, in detecting language deficits in signing children that are not the consequence of atypical or delayed language acquisition) or to diagnose and determine the intervention for sign language impairment as a result of a stroke, mental diseases or aging.
- In parent counseling, since a better understanding of the linguistic properties of sign languages would boost informed policies in this field.
- In multilingualism policies, that would integrate sign languages.

Deaf citizens and communities

Increasing the knowledge about sign languages, their history, and the history of their communities and culture will support a societal advance in many areas (SIGN-HUB Grant Agreement, Description of the Action, p. 18-19):

- Helping Deaf citizens and communities exercise their rights
- Changing the social perception of signers
- Promoting the acceptance of linguistic variation next to a standard version of a language
- Reducing the digital divide in the Deaf population

2. FAIR Data

2.1. Making data findable, including provisions for metadata

Data produced will be always provided with metadata to ease the tasks of storing and retrieval. Metadata will indicate, at least, information such as authorship, content and dissemination level, and will be easily identifiable and searchable. It is possible to suppose that a mechanism based on a set of persistent and unique identifiers will be enforced to speed up data retrieval.

The standard format for metadata for video is the Exchangeable Information File Format (EXIF). The metadata tags defined in the EXIF standard cover a broad spectrum, ranging from date and time information to camera settings, content description, information about the author, and also some non-text information such as preview thumbnail.

There are two types of video metadata: automatically collected video metadata, often directly registered from the video camera or the video maker software, and manually written video metadata providing human-conveyed information about the video content. Most of video metadata nowadays is automatically created, even though manually written metadata is growing and becoming more important. Data will be accompanied from automatic collected metadata, while simple video editing tools will give the opportunity to add manual metadata when needed.

Description provided from metadata enables easier and quicker searches among video contents and provide users more in-depth information about the desired video. In any case, human data retrieval will be eased also thanks to naming conventions, enforced as described

in Deliverable D3.2. Enforced conventions state that extra-long folder names and complex hierarchical structures should be avoided while using information-rich filenames instead. Filenames will group information of different types (e.g., title, date, version number) that should be carefully separated with visually ergonomic characters such as the underscore ("_") and hyphen. To ease the task of reading file names for humans, the first letter of each element should be capitalized. Within a filename, the elements should be ordered logically, in the same sequence that a user would normally search for a targeted file. This is also to ensure a proper chronological and alphabetical order when storing the files. This is the reason why when personal names have to appear within file names the family name should come first followed by first names or initials, while time elements should be ordered as year, month and day.

Finally, especially when files are meant to be shared, it is of relevance to set versioning and prefix mechanisms. An element for version control should be included within the file name, typically at its last most position, and should start with the "v" letter, or the "rev" code, followed by a version identifier (typically expressed in one digit) and a file identifier (typically expressed in three digits). To distinguish between drafts and final releases, version identifiers should be differentiated among, for instance, zero and non-zero numbers. Version identifiers should remain coherent and be incremented cleverly, particularly only when files have undergone major changes. Conversely, identifiers such as "new version" or "final version" should be avoided, as they could generate confusion considering than even final drafts files can be updated and modified.

2.2. Making data openly accessible

Options for data deposition in a repository are still being explored.

Data produced in Task 2.3 elicited from people with (suspected) language impairments will not be made openly available, in order to prevent the risk of enhancing vulnerability/stigmatisation of this population.

Except for individuals with (suspected) language impairments, we will ask participants if they agree that excerpts of the videos in which they appear are used in scientific publications and scientific meetings, in the documentary films about the life of elderly signers during specific moments of European history (only for elderly signers) and in the website.

The videos will then be available and accessible to everyone via a web-platform both on fixed and portable devices.

The web platform should provide content accessible to deaf people and hearing impaired people, in compliance with the Web Content Accessibility Guidelines 2.0, level AAA.

Deliverables produced during the project that can be made public according to the GA will be available through the project website. Therefore, access will be guaranteed by a web browser (Microsoft Internet Explorer, Firefox, Safari and Chrome).

Video will be produced by using formats compliant with modern web technologies. The requirements to access the videos that have been identified are the following:

- It should be able to be used in a Web browser
- Internet connection should offer a sufficient loading speed

2.3. Making data interoperable

Data produced will be released in conformity to the most known and spread standards for its representation. When possible, open standards will be chosen rather than proprietary ones, in order to maximize data interoperability, sharing and transmissions. Examples ranges from standard text files and spreadsheets conventions and data format (e.g., "XLS") for what concerns documents, deliverables and surveys, to standard video containers (e.g., "MP4") for

what concerns multimedia video content. Metadata will be represented in accordance with modern vocabularies common to researchers and institutions in different fields (e.g., the "Dublin Core Metadata Element Set"), so that it should be not necessary to define project specific ontologies.

2.4. Increase data re-use (through clarifying licences)

Personal data will be kept only for the duration of the project and will not be available to third parties: access will be restricted since these data will contain private and sensible information. Anonymized and public data (e.g., video and multimedia content) will be retained also after the duration of the project and will be made available to third parties with no embargo in terms of timing but with some distinctions in terms of modalities. In particular, visual files will not be downloadable, instead they will be available through streaming.
Public data will be released under widely used free and copyleft software license, such as the GNU General Public License (GPL).

3. Allocation of resources

The data will be stored in a dedicated web space accessible by a web interface. Therefore, it is required to purchase a sufficient amount of space by the selected web hosting provider to preserve value data for long term. The cost per year for purchasing a sufficient space is approximately 50 €.

We will clearly identify a management structure to responsibly decide how to give grant to access to the data in the future DMP updates.

4. Data security

4.1. Dissociation file

The data will be treated as requiring the highest level of protection. A dissociation procedure is established to separate the actual data from the identity of the consultants.

All data and metadata, including data and metadata about clinical populations, will only be coded, on the tests and in the excel sheets, using participant numbers, to warrant anonymity. All publications will only use arbitrary subject numbers.

All data will be kept in a locked closet within a closed room, protected by a key and digital files will be stored within a secured environment with controlled and registered access to protect them from unauthorized access. All researchers will sign a confidential commitment.

Personal data will be kept for the duration of the project; only anonymized data will be kept for future research, and participant's consent will be sought to keep and use recordings and other personal data for future research on sign languages at the same institution that collected data.

The dissociation file will contain the data to identify each person that has accepted to participate in the Project and the link to a randomly assigned and unique identifier code (id), which will be used to identify him/her in the videos and in the rest of information about him/her.

This file will be segregated from the rest of the project information. There will be a dissociation file for each partner, and it will not be shared between the partners. Each partner will be responsible for the safekeeping of his file following the security measures listed below:

- It will be accessible only by the minimum set of people necessary to carry out the project and it will not be accessible to all researchers of the project.
- The information will be stored encrypted in a portable storage device (hard disk USB or similar) usually disconnected from the net, and a backup will be done. Only personnel with the right to access information will know the decryption password.
- The hard disk will be kept in a locked closet within a closed room.
- The access to the device will be registered (day / hour / name of the person accessing it). It will consist in principle in a piece of paper that will be next to the data storage device.
- Its label will prevent external people outside the project knowing its content.
- The dissociation file will be stored at least 2 years after the end of the research.
- In principle, the transmission of the content of this file is not considered. In case of having to physically move it, only one copy will be moved (leaving the backup in the office of the participating entity) in a locked briefcase.
- Measures explained in section 4.2 will be also applied.

4.2. Data used by researchers

In this section we refer to data (videos and metadata) commonly used by researchers. There will be a central repository that will gather the information of each partner, and each partner will have a local work copy. The safekeeping of both the central and the local copies will comply with the following security measures:

IDENTIFICATION AND AUTHENTICATION

1. The measures that guarantee the correct identification and authentication of the users shall be taken.
2. A mechanism that permits the unequivocal and personalized identification of any user who tries to access the information system and the verification of his authorization shall be established.
3. When the authentication mechanism is based on the existence of passwords there shall be a procedure of disclosure, distribution and storage guaranteeing their confidentiality and integrity.
4. Passwords shall be stored in an unintelligible way.
5. A mechanism to limit the possibility of repeated attempts of unauthorized access to the information systems shall be established.

ACCESS CONTROL AND RECORD

1. Users shall only have access to those resources required for the performance of their functions.
2. It shall be ensured that there is an updated list of users and user profiles, and the authorized accesses for each one.
3. Mechanisms shall be established to avoid a user being able to access resources with rights other than those authorized.
4. Only staff members authorized shall grant, alter or cancel access to resources, pursuant to the criteria established by the data controller.
5. Should personnel not pertaining to the data controller have access to the resources they shall be subject to the same security conditions and obligations as the internal personnel.

6. Only authorized personnel shall have access to the places housing the physical equipment that supports the information systems.
7. For each attempt at access at least the following shall be stored: identification of the user, the date and time it was done, the filing system accessed, the type of access and whether it has been authorized or denied.
8. Should access be authorized, it shall be necessary to store the information allowing the accessed register to be identified.
9. The mechanisms that permit the register of accesses shall be under the direct control of the competent security officer and shall not permit their deactivation or manipulation.
10. The minimum period for storing the registered data shall be two years.
11. The security officer shall review the registered monitoring information at least once a month and shall draft a report of the revisions and the problems detected.

MANAGEMENT OF SUPPORTS AND DOCUMENTS

1. The supports and documents containing personal data shall permit identification of the type of information they contain, allow an inventory to be made and shall only be accessible by the personnel authorized in the security document.
1. An exception to these obligations shall be made when the physical characteristics of the support makes their fulfillment impossible.
2. The departure of supports and documents containing personal data outside the premises under the control of the data controller shall be authorized by the data controller.
3. Measures aimed at avoiding the theft, loss or unauthorized access to the information during transport shall be taken in the transfer of documentation.
4. Any document or support containing personal data that is to be discarded shall always be erased or destroyed, by taking measures aimed at avoiding access to the information contained therein or its later recovery.
5. The identification of the supports containing personal data that the organization deems particularly sensitive may be made using logical labeling systems permitting authorized users of such supports and documents to identify their content, and making identification difficult for anyone else not so authorized.
6. A registration system for the entry of supports shall be established permitting, directly or indirectly, the type of document or support to be known, as well as the date and time, the issuer, the number of documents or supports included in the dispatch, the type of information they contain, the method of dispatch and the person responsible for receipt, who shall be duly authorized.
7. Similarly, a registration system for the departure of supports shall be provided permitting, directly or indirectly, the type of document or support to be known, as well as the date and time, the recipient, the number of documents or supports included in the dispatch, the type of information they contain, the method of dispatch and the person responsible for delivery, who shall be duly authorized.
8. The distribution of supports containing personal data shall be done encoding such data or using another mechanism that guarantees that such information is not accessible or manipulated during transport. Similarly, the data contained in portable devices shall be encoded when they are outside the installations of the data controller.
9. The processing of personal data in portable devices that do not permit encoding shall be avoided.

BACKUP COPIES AND RECOVERY

1. Protocols for action shall be established for making weekly backup copies, at least, unless data have been updated during that time.
2. Similarly, procedures for the recovery of data shall be established to guarantee at all times their reconstruction to the original state at the moment the loss or destruction occurred.

3. Manual recording of the data shall only be done when the loss or destruction affects partially automated filing systems or processing, and whenever the existence of documentation allows for the objective to be met to which the previous paragraph refers; a justified record of this fact being made.
4. Verification shall be ensured every six months of the correct definition, operation and application of the procedures for making backup copies and for the recovery of data.
5. The tests prior to the implementation or amendment of the information systems the process filing systems with personal data shall not be done with real data, unless the relevant level of security for the processing is ensured. If tests are to be done with real data, a backup copy shall be made first.
6. A backup copy of the data and of their recovery procedures shall be kept in a different place to that housing the computer equipment that processes them, which shall in any case comply with the security measures required herein, or use elements that guarantee the integrity and recovery of the information, so that their recovery is possible.

TELECOMMUNICATIONS

1. The transfer of personal data through public or wireless electronic communications networks shall be done encoding such data or using any other mechanism that guarantees the information shall not be intelligible or manipulated by third parties.

RECORD OF INCIDENTS

1. There shall be a procedure for notification and management of incidents that affect personal data and a register established for recording the type of incident, the moment it occurred, or if appropriate, was detected, the person making the notification, to whom it was communicated, the effect derived from it and the corrective measures applied.

4.3. Data published in eRepository / Internet

Since these data will be published on the Internet, we will ensure compliance with the following security measures:

- Regarding the Open Access data, in order to ensure data security, the following issues are being taken into account in designing the web platform (see deliverable D3.1, pp. 4-5):
    - It should not allow injection flaws (e.g. SQL, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query) keeping untrusted data separate from commands and queries.
    - It should implement functions related to authentication and session management in order to avoid attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.
    - It should not allow CrossSite Scripting XSS (e.g. attackers are allowed to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites) keeping untrusted data separate from active browser content.
    - It should not allow Insecure Direct Object References in order to avoid attackers to manipulate these references to access unauthorized data.
    - Secure settings should be defined, implemented, and maintained for the platform, frameworks, application server, web server and database server.
    - It should properly protect sensitive data (for example by using safe cryptography) in order to avoid identity theft.

  - It should provide a consistent and easy to analyze authorization module that is invoked from all privileged functions.
  - It should not allow Cross-Site Request Forgery (CSRF) attacks (e.g. attacks that force a logged-on victim's browser to send a forged HTTP request to a vulnerable web application)
  - It should use components such as libraries, frameworks, and other software modules with known vulnerabilities.
  - It should redirect and forward users to other pages and websites using a proper validation.
- Only data of those participants who have signed their explicit consent to the public dissemination of their image will be published.
- Data will be published under the terms of use that avoid the use of images for any purpose other than the objectives of the project.
- If a request from a participant to remove images is received, they will be removed from the public domain.
- If public video platforms are used, suppliers will need to guarantee compliance with the safety measures listed above.

5. Ethical aspects

All work packages meet or exceed the requirements of informed consent as laid out in European and National ethical guidelines (see art. 19 of Regulation of Establishment of Horizon 2020 No 1291/2013; CNIL for France, NBC for Italy, CEIC for Spain, INBC for Israel). All beneficiaries (both EU and non-EU) confirm that the ethical standards and guidelines of Horizon2020 will be rigorously applied.

See the Description of the Action for a general introduction to the ethics issue of the SIGN-HUB project (Grant Agreement, pp. 66-67). See deliverables D5.1, D5.2, D5.7, D5.8, D5.9, D5.11, and D5.12 for ethics issues related to informed consent procedures and vulnerable individuals/groups involvement. See deliverables D5.5, D5.6 and D5.10 for information about protection of personal data.

6. DMP updates

We plan to periodically update the SIGN-HUB DMP before delivering its last version (see Table 3).

Table 3. DMP updates timetable.

Update	Event in conjunction with	Due date
1st	1st periodic report	Month 12 (March 2017)
2nd	2nd periodic report	Month 30 (September 2018)
3rd	Deliverable D1.6, full data management plan	Month 44 (November 2019)