Horizon 2020 Societal Challenge 5:
Climate action, environment, resource
efficiency and raw materials

Deliverable 3.1

Data Management Plan

Contributors:

Roberta Siciliano (UniNA), Michele Staiano (UniNA), Rafael Nebot Medina (ITC), Samuele Lo Piano (UAB), Ansel Renner (UAB), Kerry Waylen (Hutton), Alfonso Piscitelli (UniNA)

Revision history:

Date:	*Version:*	*Status/contributors:*
31 Oct 2016	v1.0	Release for technical comments / M. Staiano, R. Medina
9 Nov 2016	v1.1	Additional contributors / S. Lo Piano, A. Renner, K. Waylen
11 Nov 2016	v1.2	Circulate to consortium for final remarks
25 Nov 2016	v1.3	Integrate contribution from A. Piscitelli

Content

List of Acronyms

API: **A**pplication **P**rogramming **I**nterface;

DOI: **D**igital **O**bject **I**dentifier;

ESRI: **E**nvironmental **S**ystem **R**esearch **I**nstitute;

FAIR: **F**indable, **A**ccessible, **I**nteroperable, **R**eusable;

FAO: **F**ood and **A**gricultural **O**rganization of the United Nations;

GIS: **G**eographic **I**nformation **S**ystem;

Git: **G**lobal **I**nformation **T**racker (a version control system);

IEA: **I**nternational **E**nergy **A**gency;

IPUMS: **I**ntegrated **P**ublic **U**se **M**icrodata **S**ystem;

IPR: **I**ntellectual **P**roperty **R**ight;

MAGIC: **M**oving Towards **A**daptive **G**overnance **I**n **C**omplexity: Informing Nexus Security;

MS: **M**icro**s**oft;

MuSIASEM: **Mu**lti-scale **A**nalysis of **S**ocietal and **E**cosystem **M**etabolism;

NetCDF: **Net**work **C**ommon **D**ata **F**ormat;

OAI-PMH: **O**pen **A**rchives **I**nitiative **P**rotocol for **M**etadata **H**arvesting;

OECD: **O**rganisation for **E**conomic **C**o-operation and **D**evelopment;

PDF: **P**ortable **D**ocument **F**ormat;

REST: **RE**presentational **S**tate **T**ransfer;

SDMX: **S**tatistical **D**ata and **M**etadata **E**xchange;

TIFF: **T**agged **I**mage **F**ile **F**ormat.

List of Figures

1. Data Summary

One of the fundamental tasks in the MAGIC project is to set up a thoroughly elaborated collection of bio- and socio-economic case studies. This collection will underpin the deployment of a broad knowledge base that will eventually allow the relevant social actors – involved in a policy-assessment and policy-making participatory process – to address new case studies. To this end, all data aspects including data gathering, collection and elaboration will be performed by means of the project initiative termed the *Nexus Information Space*. It is remarked that participatory integrated assessment does not generate "a final output", rather it enables a process that is continuously producing and using information in an iterative manner. Therefore, in order to ensure a coherent engagement process with the relevant stakeholders, guaranteeing **F**indable, **A**ccessible, **I**nteroperable and **R**eusable (FAIR) data is a primary aim of MAGIC. A "case study" is the unit of work in the MAGIC project, as reflected in the data management. A case study is the analysis of the WEF-Nexus in one or more geopolitical contexts by an integrated (as opposed to reductionist) approach that implies the compilation of information from diverse sets of data and from a range of sources, arranged according to the common analytical methodology used in the project, namely the MuSIASEM accounting framework. Studies begin with a pre-analytical phase, were the case is framed or contextualized and the level of detail is roughly determined according to the information available, after which the quantitative analysis moves from the specification of a complex data structure which is elaborated and prepared for the input of extensive and intensive values (see the project glossary) that are to be obtained from external data sources. Once structure and data are specified, a set of algebraic and logical constraints are extracted and solved. The results are used to elaborate multiple types and iterations of analyses, displayable in dashboards and standalone interactive visualizations in support of the adaptive decision-making process.

Data gathered during the pre-analytical phase are mainly unstructured or partially structured documents (text, pdf, spreadsheets) and are shared by the researchers working on a given case study or related ones. The proposed storage backend – henceforth the *internal repository* – allows for the creation of *groups* sharing specific files and folders and accordingly manages secure access to them. Some of the material could be classified as *confidential data*, related to personal (e.g. transcript interviews) or other confidential information. This typology of data should be handled accordingly to the practices designed in Section 4.1 of this document. The other data may be divided primarily into two categories according to the typology of parameters provided, precisely bio-economic or socio-economic. Geo-spatio-temporal data sources are required for a geographical reference of this type of information. The relevant files are normally handled in *GIS* formats and using *GIS* protocols and tools. Socio-economic information can be built either bottom-up, from domain specific technical documents, or top-down using statistical data sources, such as *Eurostat*. Top-down statistical data typically uses the SDMX format and are standardized correspondingly.

Specifically, the list of expected formats for external sources consists of:

- GIS vector formats - ESRI Shapefiles.
- GIS raster files - GeoTIFF, ESRI.
- Excel files - For bio- and socio-economic information.
- SDMX documents - Available from statistical sources.
- Climate change scenarios - NetCDF, HDF5.
- Unstructured documents in PDF, MS Word, OpenDocument - Containing data, tabular data or formulas in a form that allows for an easy extraction of data.
- The numerical part of case studies and the underlying data structure will be persisted using a format based on JSON (currently at refinement stage i.e. the merging of a couple of initial proposals already available) or a domain specific language under development, enacted with software specifically developed for the project, that will be made available when the project is concluded on *GitHub* for open access. Textual documents that incorporate results deriving from the analysis will be elaborated using conventional office tools, with preference for open source ones.

Initial statistical data sources are (note: list is non-comprehensive in the sense that it is open to new incorporations):

- Eurostat
- FAO
- IEA
- IPUMS
- OECD
- Trademap
- UKERC

The resulting case studies are expected to be useful for diagnoses, analysis of the option space and for the quality check of current narratives about the WEF-Nexus in the process of policy making. Therefore, the case studies are of primary importance to policy and decision makers as well as other interested social agents such as citizens, NGOs and the private sector, not to mention the scientific community and the academic discourse at large.

2. FAIR Data

The progressive preparation of data for its publication complying with FAIR requirements will be based on the use of a collaborative file sharing tool that allows work to be completed within a hierarchy of folders containing files – the internal repository. In abstract, the root folders will be "public" and "confidential". The first should contain only information that can be published after a responsible decision about disclosure is made. The second will contain information whose dissemination should be restricted, such as license rights, confidentiality, or because it is sensitive or personal (see more in section 4.1). Attached to `public` there will be a `shared` folder and a collection of case study folders. The same structure will be repeated for the `confidential` folder.

```
public/
        shared/

        cs.../
                README.md
                METADATA.xml
                docs/
                        preanalytical/
                        inputs/
                        outputs/
                        analysis_of_results/
                msm/
                metadata/
        cs.../

 confidential/
        COshared/

        COcs.../
        COcs.../
```

Figure 1 - The tree of folders, with the detail for a case study

It is proposed to organize the public information on case studies using a normalized hierarchy of subfolders according to the case-studies-as-unit-of-work strategy. The special files constituting the processable core of a case study will be organized according to the MuSIASEM-data-structure specifications and serialized in a purpose-made format in the relevant subfolders. In order to comply with these data structures and annotate them with relevant metadata, a set of inputs will be compiled with different sorts of analysis: textual descriptions, charts, graphs, complex numerical and/or graphical visualizations in general, which will inherit some basic metadata from the parent folder. Moreover, a case study must include the possibility of using different MuSIASEM structures and for each of them different scenarios or families of scenarios, also for the purpose of a global sensitivity analysis. In order to cope with all these requirements, the case-study folders will be organized in subfolders according to the following predetermined arrangement of folders:

- **README.md**. A text file (in Markdown format) describing the case study.
- **METADATA.xml**. A file containing metadata extracted from the record of the case study in the GeoNetwork system, compliant with Dublin Core.
- **/docs/preanalytical**. Preliminary (unstructured) documents, properly addressing the context for the case study, serving also as base for metadata elaboration.
- **/docs/inputs**. Metadata of all inputs, and data elaborated for the case study.
- **/docs/outputs**. SDMX and spreadsheet extracts of the case study.
- **/docs/analysis_of_results.** Unstructured documents, pictures and presentations explaining different outcomes of the case study.

- **/msm**. The processable MuSIASEM data structures with references to external or internal inputs.
- **/metadata**. Metadata pieces referenced by "METADATA.xml".

Each case study makes clear at least one contact person, whose name and contact information should be included into the `README.md` file.

Common files to different case studies will be placed in a subfolder of the corresponding "shared" folder (`public` or `confidential`). Each subfolder is documented by a `README.md` file with the basic description of its contents and the contact person's information, as soon as created. References will be implemented with a text file (`LINKED_data.md`) containing link(s) to the original file(s) or folder.

Each subfolder within the first level under `public` or `confidential` folders has attached the name of the responsible person, who by default should be the creator of the folder. S/he will be in charge of adding users to the folder who can simply view or also edit its contents by choosing them by a list and setting the desired options through a simple interface of the internal repository management system. Repository administrators have no power to override this policy, so the contact person is the sole responsible for the users access rights as well as the data curation for the final publication.

Users of the internal repository who do not have access to a folder will not obviously have it listed when accessing the parent folder, therefore the repository administrator can only allow the access to the root folders `public` and `confidential`. On request of the MAGIC project manager – issued on behalf of the coordinator against any request from team leaders or case study contact person – new users may be added at this entry level. Again, it is the sole responsibility of the specific folder's contact person to allow access to it (viewing rights, editing rights).

Once a case study is ready for public re-use, the whole structure under the `public` folder will be packed and compressed using a common packaging format, such as `CSxxxyyyzzz.zip` named accordingly to the coding scheme defined in section 2.1 below. The responsible person is in charge of the inclusion into the final packaging of any referenced data in shared folders, provided s/he has determined that no infringement of confidential material or IP rights is implicated – by inquiring all other contact persons about linked data. The resulting file will then be uploaded to the public repository *Zenodo*. It is the duty of the folder's contact person to supply the whole set of data related to the case study, specifically s/he must:

- include the contact-person information and recognize authorship within metadata also for any linked data;
- attach a proper summary and an apt digest about any still confidential data related to the case study.

Therefore, the process for case-study elaboration will consist of two stages: i) **under elaboration** (internal – only people related to case study elaboration will have access); and ii) **public** (available at *Zenodo*, possibly with an embargo period according to the chosen open-access-publication scheme). During the first stage, own-project tools will be used: *OwnCloud* (soon to be migrated to *NextCloud*) instances as internal data repositories, along with *GeoNetwork* (and/or *CKAN*) for metadata management are standard tools envisioned and being tested for this purpose. Also, other specific software developed inside the project for data processing will be used. In summary, the transition from one state to the other, after review and agreement by the involved analysts, is achieved in the following steps:

- Prepare metadata file;
- Package (.zip file);
- Upload file to *Zenodo*, using the previously available metadata;
- Point DOI back to the “METADATA.xml” file.

2.1 Making data findable, including provisions for metadata

Both external data sources and case studies – the data source elaborated inside the project – will be inventoried. Case study records will be annotated with metadata following the Dublin Core generic metadata standard (having four levels of interoperability, divided into 15 sections for data description) and ISO 19139 (the latest being an implementation of ISO 19115, concerning geographic information metadata), using a tool called *GeoNetwork*.

When a case study passes from the “under elaboration” phase to the “public” phase, the study’s metadata will be exported and placed into the “METADATA.xml” file found in the root folder of the case study prior to the overall final packaging.

DOIs will be obtained when registering case studies in *Zenodo*. After successful registration, the DOI has to be specified in the project platform *GeoNetwork*.

Case studies will be named following the convention:
"CS"<number>"_<geographic scope level: "R"egional, "C"ountry, "E"urope, "S"ectoral>_<Nexus subjects: "W"ater "E"nergy "F"ood "C"limate "L"and>_<restriction level: I: 'internal', C: 'confidential', P: 'public'>-<version>.

Example: `CS1_ES_WEF_P-0.1` (Europe, Sectoral, Water, Energy, Food, Public, initial version).

The case study number will be assigned by a single person, the MAGIC project manager or his delegate, who will maintain count beginning at 1 and increasing as requested by involved researchers. If a case study is deleted, its number will not be recovered.

The approach for versioning is inspired by common software engineering practice: a new case study will be labelled with a version number with two parts separated by a dot: the first number (major version) indicates the status of elaboration of the case study. An increment will indicate a break with important details of the previous version. The second number (minor version) is for corrections/improvements somehow similarly framed.

GeoNetwork allows integration with available ontologies/thesauri in order to properly qualify the case studies. Different aspects framing the case study, for instance geographical or economical (e.g. NACE Rev. 2) may be considered accordingly.

2.2 Making data openly accessible

When no embargo period applies and a data package related to a case study has been marked as **public**, it will be made openly available. Only data gathered by partners outside of the project work plan and protected by IPR, or inside the work plan but containing confidential information (e.g. related to personal interviews), will be kept closed for privacy reasons. Only aggregate summaries will be made accessible as per the European Commission Guidelines on Open Access to Scientific Publications and Research Data in Horizon 2020. This option is typically compatible with the access scheme offered by *Zenodo*.

As described, public access to data will be made available by means of one or more *Zenodo* datasets, one per case study (*Zenodo* will automatically link to OpenAIRE). All these data will be fully accessible thanks to the included metadata and the search facility available on *Zenodo*.

The majority of the data will be shared in open-source formats. Any software tool capable of decoding data structures and developed under the MAGIC project will be released under an open source license (*EUPL, Apache, MIT, BSD-3* are suitable options) and made accessible at the end of the project by a *GitHub* repository linked to the *Zenodo* dataset. The released code will remain hosted on *GitHub* and linked into the same dataset(s) with a specific DOI, so it can be open to reuse in order to decode the datasets.

2.3 Making data interoperable

Case studies will be structured/articulated following the MuSIASEM framework, using the concepts and terms on which the methodology is based. Specifically the resulting external inputs of the data structures will reflect this through taxonomies and thesauri (standard vocabularies of GIS and/or statistical terms). Processing the MuSIASEM data structure constitutes one of the ongoing deliverables of the project. For this reason the format in which it is interchanged will be in constant evolution as new issues and opportunities present themselves. This evolution will be conveniently covered and well documented in a chronicle which also explains the basic self-containment concepts of the methodology. Static and periodical SDMX extracts of the data structure can be provided by users.

In general, any specific format used will be documented alongside an accompanying software used to process custom data structures.

Since a *GeoNetwork* node will be activated in the project, standard metadata vocabularies and thesauri (Dublin Core, ISO 19115 and ISO 19139) will be used to deploy an internal metadata system. Its implementation will be updated with any custom entry required by the project along with a suitable mapping to common ontologies. At the same time, this guarantees an easy and safe handling of geographic data.

2.4 Increase data re-use (through clarifying licenses)

Data published inside MAGIC may be reused by people related to the many areas covered by the project: social, economical, political, environmental, technological as well as persons in academia.

For any data piece requiring a license, the default proposal is: Creative Commons Attribution-Non Commercial-Share Alike 4.0 International (CC BY-NC-SA 4.0):

cc BY NC SA

Data will be treated on a case study basis during the project, i.e. case studies under development will be kept accessible only to project partner team members until the setup, calculations, audit, revision and other checking phases (included checking any pending third party intellectual property rights) are completed and disclosure is authorized by the coordinator. Once made publicly available on *Zenodo*, cases will be fully reusable (with the possibility of specifying embargo period or with controlled access to whitelist of persons; see: https://www.zenodo.org/policies).

Data collected and produced by the project may be reused by people included in the project initiative termed the *Nexus Dialogue Space*. Once the data is made publicly available, anyone is entitled to re-use them. All the data disclosed to the public will be re-usable.

The concept of *data pedigree* adopted in the project will assure that each piece of relevant information is traceable back to original data sources. This data lineage along with metadata allows for quality audit and sensitivity analyses of the outputs to be carried out inside the *Nexus Information Space*. Suitable procedures will be defined to sustain these processes in the foregoing editions of the DMP.

The data will remain re-usable until *Zenodo* discontinues the dataset(s) (i.e. warrantied for a minimum of 20 years).

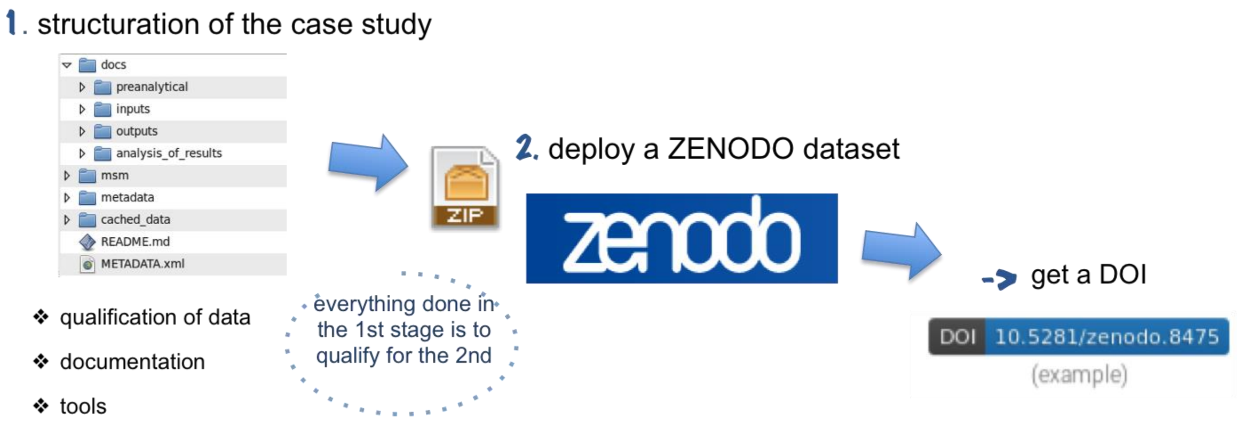

Figure 2 - The process of minting a DOI for a case study

3. Allocation of resources

As this preliminary DMP is currently based on the use of free resources and open source software, the only costs that will be incurred are related to the server(s) (hardware) required to run them and the working time needed to setup, maintain and evolve the different tools (efforts measured by person/months). Dedicated financial resources have already been singled out in the project budget description.

Michele Staiano (UniNA) and Rafael Nebot Medina (ITC) are in charge of the DMP – from the scientific and technical perspectives, respectively. Their duties include the first version release by M6 and the regular update at the intermediate reporting periods (M12, M30 and M48) or whenever a significant change takes place (new kinds of dataset creation, changes to the policy about openness and so forth). They also take the responsibility of delivering at least an initial training webinar (in order to offer to project partners a tutorial to cope with the duties in the DMP) and to maintain a FAQ section on the internal collaborative platform (*Wiki* or *Trac* system, useful to collect feedback about use cases).

Mario Giampietro (UAB, Project Coordinator) will monitor the proper execution of the plan.
The case-study leaders are to follow the plan specifications, adopt the practices prescribed and the software tools provided and finally disseminate them through their team.

As *Zenodo* will be used for long-term preservation, no related costs are on project budget.

The potential value of long term preservation of the data produced in the MAGIC project is bound to three dimensions:

- **Reproducibility** and **transparency** – some of the outcomes expected from the project are relevant not only to the academia (allowing peers to review and re-use the data so to enhance *reproducibility* of the scientific results), but also are intended to support policy making as well as to be disclosed to citizens. This calls for *transparency*. Transparency is not only about access, it is also about sharing, re-use for discussion and in support of scenario analyses by policy makers and stakeholders, who should both be enabled to understand, analyse and visualize the material. All this is possible by making the material openly accessible.

- **Releasing social** and **scientific value** – by opening up data, MAGIC contributes to driving the spread of innovative approaches to governance, delivering social and scientific value.

- **Participation** and **engagement** – the participatory approach which inspires MAGIC asks for engaging policy makers, stakeholders and public audience toward governance of the nexus security. Nowadays citizens are only able to sporadically engage with their governing bodies. By opening up data about the WEF-Nexus, citizens will be enabled to become much more informed and also to become directly involved in decision-making. The value on this dimension is somewhat intangible, but adds significantly to transparency by enabling the move towards what is referred to as a *full "read/write" society*. In such a society citizens not just know *ex post* what happened in the process of governance, but are actually able to contribute to it.

4. Data Security

A simple local backup mechanism will be guaranteed during the project lifespan in order to save the information kept by the different tools implementing the DMP.

The server hosting the tools will be accessible only by authorized system administrators. Files containing confidential data should be protected by owners using local encryption tools (i.e. password-protected archives) before being uploaded to shared repositories – see section 4.1 below. Interaction through web user interfaces will use *https* protocol (i.e. secure). Also, a secure file transfer protocol (*ftp*) will be provided as the need arises.

4.1 Protocol for confidential data

Specific rules for the handling of *confidential data* have been agreed upon and will be applied within the Consortium.

This protocol applies for *personal data* so long as some part of its information produced and exchanged for the sake of MAGIC tasks is marked as *confidential*.

- Confidential data are defined into the art. 36 of the MAGIC G.A. (see p. 54 Grant Agreement Number 689669).
- Personal data likely to be handled in the MAGIC project are included into surveys, recorded interviews or the related transcripts (see section 5.1) and they should be treated accordingly to the same practices here established for confidential data.

Both kinds of data should have one person responsible (for the confidential data by default is the one who marks them as such) and a contact person (the two could coincide).

The responsible and contact persons' information should be clearly attached to any *container* (folder or archive, in the form of a *.zip file) they are stored in from within the README.md file in the root of the container tree folder. The responsible person's role is set accordingly to art. 2 in EU Directive 95/46/EC. S/he is in charge of assuring a twofold layer of security about the data:

- the first layer of security concerns to whom s/he gives access to the shared internal repository (the sharing mechanism adopted in the *OwnCloud* repository is the personal authorization of known users of the repository, not the shared link that administrators will keep disabled, and no user is extended the authorization to share further i.e. the *re-sharing* mechanism will be kept disabled);
- the second layer consists in setting and sharing a passphrase to access the single file or archive.

Passphrases should be set accordingly to good practices – see the following box – and not exchanged by mean of the link (e.g. file link through email – *OwnCloud* is able to automatically notify users about sharing and passphrase through text message – by phone or Skype) and kept safe.

Recommended rules for a good password

Has 12 characters, Minimum: One must choose a password that's long enough. There's no minimum password length everyone agrees on, but you should generally go for passwords that are a minimum of 12 to 14 characters in length. A longer password would be even better.

Includes Numbers, Symbols, Capital Letters, and Lower-Case Letters: Use a mix of different types of characters to make the password harder to crack.

Isn't a Dictionary Word or Combination of Dictionary Words: Stay away from obvious dictionary words and combinations of dictionary words. Any word on its own is bad. Any combination of a few words, especially if they're obvious, is also bad. For example, "house" is a terrible password. "Red house" is also very bad.

Doesn't Rely on Obvious Substitutions: Don't use common substitutions, either — for example, "H0use" isn't strong just because you've replaced an o with a 0. That's just obvious.

The responsible person obtains assurance that each other person with access to confidential data agrees to be committed with the same good practices to keep confidentiality by referring her/him to this section of the Data Management Plan.

For instance, everybody entitled to access and store locally the confidential data would not share the data with people other than the ones agreed upon with the responsible person and assuming the responsibility to adopt similar means to protect data confidentiality (i.e. keeping the data containers protected by password inside a personal account directory tree without copying them in shared folders or external storages facilities nor uploading to any other repository. Analogously, any backup or hard copy should be stored in a locked closet or drawer in own room/office).

These procedures are designed, set and applied in order to fully comply with privacy issues as ruled by EU Directive 95/46/EC (see also section 5 of this document).

5. Ethical Aspects

MAGIC will both collect and process personal data in the form of surveys, recorded interviews or related transcripts. Some of this will be collected by use of electronic audio recording devices (dictaphones). EU Directive 95/46/EC considers political opinions as sensitive personal information. Given the topic of the research, information provided by participants may include political views in the broader sense. However, it is not anticipated that data on other sensitive issues such as religion, ethnicity, health or sexual orientation will be collected. No data transfers to other countries will be required. All these data, both qualitative and quantitative and including the audio recordings, must be securely stored and managed to protect identities and privacy, and in accordance with the latest versions of legislation in the EU (e.g. Directive 95/46/EC). As foreseen in the Grant Agreement, high end standard technologies will be adopted in order to safely assure the privacy of any personal data stored in electronic form (see Section 4.1).

5.1 Informed consent for collection and use of personal data

MAGIC will seek fully informed consent in advance of the data collection for any research activities. This consent must be given voluntarily by the participants, without coercion.

Before seeking consent, the research team will provide a project information sheet. The factsheet will (i) summarise the aims, methods and implications of the research along with the expected recipients of the study, (ii) make clear that the nature of the participation that is asked of the individual, (iii) explicitly state that participation is voluntary and can be withdrawn at any time without personal consequences, (iv) highlight the rights to access and ask for correction of personal data and (v) provide links to further information including the responsible person's and the contact person's email addresses. The participants will be notified of these fundamentals and any other essential information required to fully comply with art. 10 in EU Directive 95/46/EC. Before signing the form, team members will extend the opportunity to ask questions to participants.

MAGIC favours the use of written informed consent i.e. via signing a consent form, but where interviews are being audio-recorded (i.e. for telephone interviews in activity X) participants will be given the option to indicate consent verbally on the digital recording as an alternative to signing the form: if this occurs, the recorded consent will be safely stored with the forms. For workshops whose discussions outputs will feed into the research, information about the meeting and consent will be discussed in plenary at the start of the meeting. In these venues, participants will be asked to inform the research team, either publically or privately, if they wish to opt-out of having their material used in MAGIC. Records of informed consent will be stored safely along with other personal data collected by the project (see next section).

5.2 Storage and processing of personal data

Participants' personal data will be recorded in order to facilitate the research analysis, but this will be kept confidential to the MAGIC research team, stored in accordance with the provisions of the 95/46/EC Directive (including its revisions) and handled as established in section 4.1 for the sake of statistical analyses carried out by electronic means. The published outcomes of the analyses should report only aggregated summaries of the data and by no way will it be possible from the results to personally identify any of the participants. In particular, personal data (such as contact addresses of study participants) will be stored in password protected files (or in locked cabinets, in the case of any non-digital data). Only MAGIC team members will have access to the project folders and files used to store and manage data.

All personal data (whether textual or visual) will be anonymised in all outputs and reporting, e.g. by using pseudonyms during the analysis and presentation of qualitative data. Policies and any specific cases discussed will be identifiable, but individuals will not be, unless explicitly agreed or requested otherwise. The most likely situation when this may occur is if policy-makers and other stakeholders wish join a discussion forum to share ideas with others. If this is the case, the group will be 'opt in' rather than 'opt out'. All outputs will acknowledge the inputs of those who agreed to be interview, but these acknowledgements will be anonymised unless expressly agreed otherwise. Personal data will be kept in a form which permits identification of individuals for no longer than is necessary for the purposes of the MAGIC project. At the end of the project these data will be destroyed or properly detached of any sensitive information; conversely the appropriate safeguards for longer period storage for historical, statistical or scientific use are the responsibility of the partner institution the responsible person belongs to.

Finally, MAGIC consortium members' intellectual property and contributions to the research will be recognised in authorship of academic and non-academic publications.

6. Other

Once the data are transferred among team members – strictly following the practices for the protection of personal and confidential data sets in this Data Management Plan – who are based in a different Member State, the responsible person must designate a representative established in the territory of that Member State in charge of assuring that they are handled in full compliance with any more stringent rules in force at the national level. In analogy, the same principle applies with regard to any regulations set internally by the institution or department one of the project partners belongs to or is based.

Annex 1

The DMP Tutorial (draft for the webinar sessions) is made available by the following link:
https://drive.google.com/open?id=0B1cx5y814A8IWWgtekFOenl6VGc