HORIZON-MSCA-2022-SE-01-01
(MSCA Staff Exchanges 2022)

This project has received funding from the European Union's HORIZON.1.2 - Marie Skłodowska-Curie Actions (MSCA) programme under grant agreement ID 101131481.

distributed ledger technologies and user-driven automation towards self-SOVEREIGN mobile data access in beyond 5G networks

SOVEREIGN

WP2– System Architecture, Requirements and Data

Deliverable D1.1 "Data management and research output management plan"

Editor(s):	John Vardakas (IQU)
Author(s):	Jogn Vardakas (IQU), Dionysis Xenakis (UOA)
Dissemination Level:	**Public**
Type:	**DMP**
Version:	1.0

Project Profile	
Contract Number	101131481
Acronym	SOVEREIGN
Title	distributed ledger technologies and user-driven automation towards self-SOVEREIGN mobile data access in beyond 5G networks
Start Date	January 1st, 2024
Duration	48 Months

Document History

VERSIONS

Version	Date	Author	Remarks
Version	Date	Author	Remarks
0.1	25/04/2024	John Vardakas	Initial draft
1.0	30/6/2024	Jogn Vardakas	Final version

Executive Summary

This deliverable presents the data management plan to be followed in the project. More specifically, it describes the FAIR data management procedures, the online repository that will be used for the storage of the different shared files/datasets in the context of SOVEREIGN, the different data sources of the SOVEREIGN, along with the document files that will serve as databases for the employed datasets. Finally, it provides details about the access policies for the different SOVEREIGN outcomes (i.e., deliverables, scientific publications and source code) and explains the data management processes and IPR issues, together with details about the compliance of the SOVEREIGN with the GDPR.

Contents

Executive Summary 3
Table of Figures 4
Table of Tables 5
1 Introduction 6
2 Open Science and Open Access 7
2.1 FAIR Data Principles 7
2.2 Open-access to Research 8
3 Data repository of Sovereign 8
4 Research Data 8
4.1 Access to existing data sets 9
4.2 Data provided by SOVEREIGN partners 9
4.3 Data generated in the context of SOVEREIGN 10
5 SOVEREIGN outputs 11
5.1 Public deliverables 11
5.2 Scientific publications 11
5.3 Open source software 11
6 Data management issues 11
6.1 Data archiving issues 11
6.2 IPR management 12
6.3 Legal and Ethical Obligations 13
7 Compliance with General Data Protection Regulation (GDPR) 14
8 Conclusions 16
References 17

Table of Figures

No table of figures entries found.

Table of Tables

Table 1: Comparison of localization technologies 9

Table 2 Required information for data provided by SOVEREIGN partners... 10

Table 3 Required information for data generated in SOVEREIGN 10

1 Introduction

SOVEREIGN is a 4-year research project research programme sets the ambitious aim to design, implement, and experimentally demonstrate the performance of an innovative end-to-end B5G service platform that natively integrates DLTs and artificial intelligence (AI) optimizations into the B5G service chain towards fully decentralized, instantaneous, and anonymous resource trading across the B5G network ecosystem (end terminals, infrastructure, OTT service providers, etc.). In addition, there is a technical task (Task 6.2: Platform assessment/optimization on real-life use cases) including real-life assessment by academic students and industrial clients of the SMEs. On top of this, there is also the possibility that SOVEREIGN consortium members will provide data to be used in the project.

The structure of this deliverable is as follows: Section 2 describes the FAIR data management procedures, Section 3 describes the online repository that will be used for the storage of the different shared files/datasets in the context of SOVEREIGN. Section 4 describes the different data sources of the SOVEREIGN, along with the document files that will serve as databases for the employed datasets. Section 5 provides details about the access policies for the different SOVEREIGN outcomes (i.e., deliverables, scientific publications and source code). Section 6 explains the data management processes and IPR issues, while Section 7 provides details about the compliance of the SOVEREIGN with the GDPR. Section 8 concludes this deliverable.

2 Open Science and Open Access

2.1 FAIR Data Principles

The Guidelines on Data Management in Horizon Europe highlight the paramount importance of ensuring the Findability, Accessibility, Interoperability, and Reusability (FAIR) of data generated through funded projects. These guidelines aim to establish robust data management practices that enable effective handling of research data. Specifically, adherence to FAIR principles involves employing standardized formats and metadata to enhance data discoverability, clearly defining data sharing protocols and determining which data will be openly accessible. Additionally, it encourages the use of open repositories for data exchange and focuses on facilitating data reusability. Considering these objectives, the subsequent sections of the Data Management Plan (DMP) outline the approach employed within the SOVEREIGN framework, encompassing strategies for achieving data findability, accessibility, and interoperability, as well as ensuring data preservation and open access to maximize its potential for reuse.

Findability: SOVEREIGN consortium partners are committed to use the European Open Science Cloud and the Open Research Europe [1] scholarly fully open access publishing service for HEU to enable rapid publication data that support research integrity, reproducibility, transparency and enable open science practices. Encouraging a transparent, open source and open innovation culture, SOVEREIGN will make accessible its SW repositories through well-known trusted repositories for distributed version control and source code platforms, such as GitHub [2] and GitLab [3]. The project repository can be concentrated in reference sites, such as Stack Overflow [4], the largest, most trusted online community for developers to learn and share knowledge. Different types of persistent identifiers for digital objects will be used, such as Archival Resource Keys, Electronic Identifier Serial Publications, Digital Object Identifiers, Uniform Resource Names, Persistent Uniform Resource Locators, etc.

Accessibility: The Consortium Agreement defines the details concerning the access rights for exploitation to background and results.

Inter-operability: Standards: ISO/IEC 20547-4:2020 [5], NIST SP 1500-4r2 [6]. Formats: Data collected will be used for raw measurements (e.g., timestamps), which will be stored in plain text format, such as comma separated values (CSV-like). The scripts used to analyse the data will be stored in their respective source code formats. Logs that contain the history of the state of various processing elements will be stored in plain text format. Artifacts such as plots generated through analysis will be stored as plain or vector images. Data traces and SW source codes in numerical and text formats. All data gathered from involved end-users during the co-design process and the demonstrations will be pseudo-anonymised prior to processing, to ensure GDPR [7] compliance.

Reusability: SOVEREIGN provides added value to the European research community by promoting open-source code. Part of the work of SOVEREIGN SW development partners will involve the use of either Open-Source code in their deliverables or contribute their deliverables to open-source communities. Creative Commons licenses [8] will be used for sharing research data and academic publishing and, CC-BY (By Attribution) license for open access papers, which permits sharing and reuse of the material for any purpose if the original authors are credited. These licenses will be applied to items uploaded to the European OpenAIRE [9] Research Data Repository. Well-known tools/SW, such as Datprof [10], EMS Data Generator [11], Redgate SQL Data Generator [12], CA TDM [13], etc., will be used for data generation, validation, interpretation and re-use.

2.2 Open-access to Research

SOVEREIGN consortium partners are committed to use the Open Research Europe open access publishing platform for scientific articles to enable rapid publication times and publication outputs that support research integrity, reproducibility, transparency and enable open science practices. The project has dedicated part of its budget to cover the fees associated with open-access publication to facilitate dissemination and reuse of the project's results. Project participants, for various reasons, may need to submit articles to journals (or proceedings) that only offer a lower level of open access, requiring either parallel publication or an embargo period. The need for this will be evaluated on a case-by-case basis and benefits will be balanced against the less convenient or delayed access to the result. In any case, the final author's version of every accepted paper will be made publicly available, in accordance with the rules posed by many journals. Consortium partners will also use self-archiving (or green open access) services for research community, such as Zenodo [14], OpenAire [15], ResearchGate [16] or Academia [17], that will allow balance between traditional publications and open-access.

3 Data repository of Sovereign

The project coordinator, UoA, has set up a shared space as a data repository for the SOVEREIGN project. Google Drive, an online tool, fully compliant with all the security and General Data Protection Regulation (GDPR) [7] requirements, will be used as the project data repository for the duration of the project. The project data repository will be used by the partners as the primary location for uploading and storing files related to the SOVEREIGN project, such as Deliverables, Meeting Minutes, Workshop Photos and other working documents.

All project partners have access to Google Drive which is dedicated to SOVEREIGN. Users/persons outside the consortium can't have any access to this dedicated space. The access rights are granted after communication with the project manager that supervises this tool and grants access rights to Google Drive. Users, after login (user and password pair), are navigated to the home page of the Project. See below a screen shot of the environment.

4 Research Data

SOVEREIGN is a research project that is heavily based on the use of data as its technical part is focused on data-driven solution. In this context, it is expected that several existing datasets will be exploited, while new 6G-oriented networking data will be also generated through the foreseen Proof-of-Concepts (PoCs) and use cases throughout the project. Indicative types of data include aggregated network data per flow/service provided to the platform to enable its proper functioning, aggregated network data about flow/service of network data gathered, detailed data traces collected for specific purposes, software source codes, technical reports and manuals. In this section, we present the plan for accessing external data sources, as well as the framework for the data generated in the context of SOVEREIGN.

4.1 Access to existing data sets

Table 1: Comparison of localization technologies

Dataset Name	Description of dataset	Owner/Source	Access Considerations
Scientific publications	Journals/Magazines, books, conference proceedings, etc.	Publishers such as IEEE, Elsevier, ACM, Springer and others.	Available at a cost based on unit purchase or subscription basis.
Open Access Scientific Publications	Online open access scientific publications.	Respective copyright holders, such as publishers and authors.	Available free of charge on the Internet.
IETF drafts and RFCs	Working documents of the Internet Engineering Task Force.	IETF Trust and the persons identified as the document authors.	Available free of charge on the Internet.
3GPP	3GPP Specifications and Working Drafts of various working areas.	The 3GPP Organizational Partners jointly own copyright on the Technical Specifications and the Technical Reports approved by 3GPP.	Free of charge – published up to four times a year.
TM Forum Standards	TM Forum standards and technical reports.	TM Forum.	Available at a cost based on unit purchase; free for TM Forum members.
ETSI Standards	European Standard (EN), ETSI Standard (ES), ETSI Guide (EG), ETSI Technical Specification (TS), ETSI Technical Report (TR), ETSI Special Report (SR), ETSI Group Report (GR), ETSI Group Specification (GS)	ETSI and authors of working drafts.	Available at no cost on the Internet. Working drafts available for members.
Open Source Project Repositories and associated Project Sites	Code repositories maintained e.g. on GitHub, Google code and other places.	Depends on Open Source license used.	Available free of charge on the Internet.

4.2 Data provided by SOVEREIGN partners

SOVEREIGN consortium includes both academic and industrial partners who have access to real data and it is possible to provide part of these data to the consortium. To guarantee the proper tracking and storage of these data, the following fields should be completed for every given dataset. It is worth noting that thorough sanitization processes will be performed to guarantee the anonymization of the provided data.

Table 2 Required information for data provided by SOVEREIGN partners

Field	Explanation
Dataset reference and name	Identifier for the dataset to be produced
Dataset owner	Identifier for the data beneficiary partner
Dataset description	Origin (in case it is collected), scale and to whom it could be useful, and whether it underpins a scientific publication. Information on the existence (or not) of similar data and the possibilities for integration and reuse.
Standards and metadata	Reference to existing suitable standards of the discipline. If these do not exist, an outline on how and what metadata will be created
Confidential (Y/N)	Indicates if the data should be treated as confidential on not.
Sanitization (Y/N)	Indicates whether a sanitization process has been applied for the data anonymization. The specific process will be also identified if possible.
Link	Link to the online repository where data are stored
Contact Person	Name, email and affiliation of the dataset owner representative

4.3 Data generated in the context of SOVEREIGN

Besides the data that will be exploited either by online sources or partners´ contributions, it is also expected that data will be generated thanks to the technical work packages of SOVEREIGN. In particular, SOVEREIGN includes specific tasks that focus on data generation, while service platform integration, assessment & testing in WP6 can also generate important data to be exploited by the consortium. In case of generation of new datasets, the involved beneficiaries should also fill the respective table, which includes the following information.

Table 3 Required information for data generated in SOVEREIGN

Field	Explanation
Dataset reference and name	Identifier for the dataset to be produced
Dataset owner(s)	Identifier for the data beneficiary partner(s)
Dataset description	Origin (in case it is collected), scale and to whom it could be useful, and whether it underpins a scientific publication. Information on the existence (or not) of similar data and the possibilities for integration and reuse.
Standards and metadata	Reference to existing suitable standards of the discipline. If these do not exist, an outline on how and what metadata will be created
Relevant Task/WP	The Task/WP that generated the dataset
Confidential (Y/N)	Indicates if the data should be treated as confidential on not.

Sanitization (Y/N)	Indicates whether a sanitization process has been applied for the data anonymization. The specific process will be also identified if possible.
Link	Link to the online repository where data are stored
Contact Person	Name, email and affiliation of the dataset owner(s) representative(s)

5 SOVEREIGN outputs

5.1 Public deliverables

The list of deliverables is included in the Grant Agreement no: 101131481 for the SOVEREIGN project. The deliverables with dissemination level “Confidential” will be made available only to the consortium members (including the European Commission services). On the other hand, public deliverables produced by SOVEREIGN will be made publicly accessible and available via the SOVEREIGN website at a designated deliverables section

5.2 Scientific publications

A list of planned scientific publications can obviously not be provided in this document, since the scientific publications depend on the acceptance of the scientific submission to the respective journals and conferences. A list of successful submissions will be provided online at a dedicated location on the project website and reported through the EC project management portal. In addition, all consortium members should follow the OpenAIRE guidelines for open access publications and upload the pre-published accepted versions of their publications in open access tools, such as ArXiV[1] or Zenodo[2]. The partners are committed as per the GA to provide the open access links in the EC project management portal.

5.3 Open source software

With regard to the use and contributions to open source initiatives, the consortium will follow strictly the license terms of the open source product in question. Project partners have been working with open source software for many years and are well aware of incompatibilities occurring when different open source licenses are combined, with or without own proprietary code. The main open source initiatives considered by SOVEREIGN, for example Open Source Mano (OSM) and Open Air Interface (OAI), have released their code under exploitation-friendly licenses. Contributions to the code base of such projects will follow the target license terms. SOVEREIGN does not plan to create a proprietary open source project, hence there is no need to decide an open source license or define new license terms. In case an open source project is created, this document will be updated accordingly.

6 Data management issues

6.1 Data archiving issues

All project related documents (raw formats), deliverables, reports, publications, data, and other

[1] https://arxiv.org/

[2] https://zenodo.org/

artifacts will be stored in an online cloud repository accessible during the project for all partners. This repository will be hosted (with backup) by the coordinator University of Athens (UOA) and the link will be distributed to all project partners. Access to the repository will be given to registered persons from project partners only. The folder structure of the repository will be managed by the project coordinator (UOA) and changes of the structure need to be coordinated with the coordinator. Corresponding partners will keep the above-mentioned repositories operational during the project lifetime. After project closure, repositories will be maintained for at least one more year. After project closure the administrating partner can change access policies (e.g., restricted access / access on demand) in order to keep maintenance costs at a minimum.

The Data Management Plan (DMP) is maintained by the Project Management Team (PMT). Since SOVEREIGN is liable for “Open Access to Research Data”, PMT members reviews of the DMP are a regular agenda item of PMT meetings, conference calls, and work package (WP) results will be checked with respect to relevant information for the DMP. The sole purpose of the DMP is how to handle the research data within the consortium.

WP leaders (WP2-WP6) are responsible for the results of tasks within their work package being aligned with the definitions in the DMP. WP leaders are also responsible for the upload of the data to the cloud as soon as they are created within their WP, while the data owners are responsible for updating the respective data set information as described in section 3.

In order to ensure that this DMP is implemented and followed, reviews (by PMT) of all kinds of project related documents (e.g., reports, deliverables, publications) will include also a check for used data and the proper documentation and use in-line with this DMP.

In case the contact person for data is leaving the project, the affiliation of the original contact person will take over the responsibility of assigning a new contact person.

6.2 IPR management

Given the strong exploitation potential that SOVEREIGN presents, consortium partners have followed a series of steps to ensure the protection of the newly generated Intellectual Property (IP), as well as their background. Furthermore, partners have agreed on the project’s exploitation strategy, as it was described in the above paragraphs. A consortium agreement has been achieved on confidentiality measures, data management, IPR management and joint ownership. The IPR management will handle the following issues:

- Protect the pre-existing know-how and information related to the use of knowledge owned by individual partners from work carried independently of the SOVEREIGN project. It is important to guarantee confidentiality on any information disclosed by the partners during the project development. The partners have been asked to specifically designate in the Consortium Agreement (CA) their Background to be provided during the implementation. Any material not expressly listed in the CA, will be deemed as excluded from the Background. The partners may require the acceptance of specific license terms in order to grant access rights to the Background.

- Protect IPR of any knowledge gained within the SOVEREIGN project. Each participant who has developed some innovative contribution within the project shall formally notify the project coordinator on IPR issues, including any special requirement for the use of this IPR in addition to or deviating from the standard IPR-rules. For avoidance of doubt, under standard IPR-rules the party creating the IP shall be the sole owner of the associated IPR. The other project partner will be notified, and a time margin will be allowed to raise any objections against the IPR statement. If no objections are raised, the IPR shall be granted; otherwise, the PMT will initiate any necessary processes to resolve the conflict of interests.

- Access to the knowledge generated within the project will be granted royalty-free to the SOVEREIGN partners for the execution of the project.

- A record of all IPR and licensing issues within the project will be kept and clear procedures for the access and use of this knowledge will be set.

- Define the exploitation potential of the obtained results and decide to disseminate or protect.

- Define a contingency plan to ensure access to project's crucial knowledge if a partner with specific IPRs leaves the consortium. Policies for the partial/full ownership transfer of results between partners have been defined in the CA.

6.3 Legal and Ethical Obligations

All SOVEREIGN partners are firmly committed to the success of the project, and their managements have supported this involvement. The consortium takes the firm commitment to comply with existing laws, namely the ones concerning copyright, IPR, and related ones. Confidentiality and IPR handling: the partners will respect the confidentiality of facts, information, knowledge, documents or the other matters communicated to them as confidential. A CA, as drawn by a committee composed of the coordinator and representatives of each partner and agreed upon by the legal departments of the partners, has been concluded between the partners. This will define in detail their rights and obligations with respect to carrying out of the Project's plan with specific regard to confidentiality and IPR handling.

In addition, to fulfil the ambitious project's objectives, the SOVEREIGN consortium coordinates directly with telecom operators, leading telecom vendors R&D, world leading ICT & telecom solution providers and SMEs. Consequently, in SOVEREIGN, ethics refer to the involvement of human beings in the research process on the one hand, and the processing of personal data throughout the project's lifetime on the other one.

The consortium is fully committed to adhere to the highest ethical, fundamental rights and legal standards, as recognised at the European Union and International levels, including the Charter of Fundamental Rights of the EU (2000/c 364/01), the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) and The European Code of Conduct for Research Integrity. The research will be conducted basing on the following ethical ground rules:

- Reliability in ensuring the quality of research, reflected in the design, the methodology, the analysis and the use of resources.

- Honesty in developing, undertaking, reviewing, reporting and communicating research in a transparent, fair, full and unbiased way.

- Respect for colleagues, research participants, society, ecosystems, cultural heritage and the environment.

- Accountability for the research from idea to publication, for its management and organisation, for training, supervision and mentoring, and for its wider impacts.

In addition, concerning risk management and legal compliance, all participants to the project are aware of their obligations as potential data processers (where appropriate), as well as issues beyond data and information protection and privacy described above. Actions will be taken to ensure that those handling subjects identifiable or sensitive information are made fully aware of their responsibilities and obligations to respect confidentiality in compliance with market standards (e.g.: ISO/IEC 27001:2005), best practices and legal requirements under the GDPR. In addition to the more general and EU wide guidelines, partners will adhere to and respect national regulations and laws. All partners are aware of their responsibilities in that sense and will follow the established rules.

7 Compliance with General Data Protection Regulation (GDPR)

Despite the fact that the SOVEREIGN project does not use any direct personal data (in the form of data coming out or processed during its research activities), it recognises the needs for creating some process related policies so that there is overall agreement of the usage/storage/retention/opt-out etc. of data from every-day (day-to-day) project activities. A list of such matters is included below where the means that the consortium will tackle them reflects the whole consortium agreed approach. It is worth noting that all personal data management processes comply with the policy and legal requirements of the EU General Data Protection Regulation (Regulation EU 2016/679, the “GDPR”), as in effect since 25 May 2018 .

1. SOVEREIGN Mailing List

Due to the size of the project, there is no need to individual mailing lists for each work package for those partners who wish to remain informed of specific work package activity. One general mailing list for all of SOVEREIGN activities and exchange of information is considered sufficient. The participants consent in providing their names and email addresses for internal project communication. Additions or removals to the mailing list are managed directly by the project coordinator (UOA). The purpose of this list is to keep a well organised list of contacts for the SOVEREIGN communications and access is restricted only to SOVEREIGN consortium partners. The mailing list will be erased and no longer maintained after the project end. Any person has the right to opt out of this list by direct email to the project coordinator.

2. Meeting-related Material

This relates to any document created and used for the purposes of project meetings. This may relate to agendas, presentations, minutes, signature lists or any other internal document created for the purposes of SOVEREIGN meetings. All these documents will be created and maintained for internal purposes of SOVEREIGN and only SOVEREIGN partners will have access to them at the SOVEREIGN cloud server in the Meetings folder. They will be kept for more than 5 years after the project end. Any person has the right to opt out of being mentioned in these by direct email to the project coordinator before or after the meeting.

3. Workshop/Conferences and Training Sessions

These data relate to the creation of workshops, agendas, programmes, participants’ lists, etc. and in general dissemination material related to SOVEREIGN organised workshops. Regarding the external publication of this material, we consider that this material can be fully anonymized if required so that it excludes personal information from the presenters/participants in the related programmes/agendas that will be shared publicly. For the parts of the related material that will be used for the workshop organisation internally to SOVEREIGN, the related files will be stored in the SOVEREIGN cloud server. The data will be kept for 5 years after the project. Any person has the right to opt out of being mentioned in these by direct email to the project coordinator before or after the event.

4. Reporting

Reporting refers to internal and external documents including SOVEREIGN progress of activities, technical overviews, etc. Related files will be including documents (reports with no personal identifiable information) and financial data sometimes including personal data. The purpose of these data is financial so that partners can claim budget requests for their related effort in SOVEREIGN. Financial data will be maintained by the project coordinator (or their specified proxy) and stored in a secure server. These (per partner) data are not to be shared with anyone internally or externally to SOVEREIGN, will be kept for more than 5 years after the project end and will be deleted after this date. Opting out of this data will be possible but will require updated financial data to be submitted by the project partner.

5. Deliverables, internal documents and other SOVEREIGN reports

During the SOVEREIGN project run-time, a large series of documentation and reporting will be provided related to the project deliverables and/or internal documents, etc. These files will be used for the project contractual obligations and shared to: SOVEREIGN partners, EC, everyone (depending on deliverable type). In these documents, the name or email of authors may be included. Following this, as far as the internal (to SOVEREIGN) and EC distributed documents are related, they will be used only for the purposes of reporting and stored in the SOVEREIGN cloud server under the deliverables section. Reports that will be shared publicly (public deliverables) will mention only the contributors, the partner name and not any other personal information. All reports will be kept for more than 5 years after the project end.

6. Usage of cookies (in SOVEREIGN sites)

In the cases that in any SOVEREIGN application (web) the usage of cookies is needed, a related pop-up window informing the user must be present, prompting the user to accept (or not) the conditions under which her/his personal information is stored. SOVEREIGN will maximize efforts to reduce the usage of cookies in its web developments.

7. Project related research data

Any personal information in data circulated internally to SOVEREIGN for research purposes (e.g., research data that have been acquired as explained in the previous sections) must be fully anonymized by the data owner and not relating in any case to personal information as stated in the chapters above.

8. Any other SOVEREIGN related data

In case that personal information needs to be added in any other document in SOVEREIGN, the project coordinator will have to notify the data owners of their personal details being included into the related document, purpose, retention, storage etc.

8 Conclusions

This deliverable has described the SOVEREIGN data management plan to be adopted in the project. It includes a detailed overview of the data that will be created, processed or utilized inside SOVEREIGN with details on the type and nature of the data managed by SOVEREIGN partners. This is a living document that will be updated (if necessary) with additional information on the data management procedures.

References

1. https://open-research-europe.ec.europa.eu/
2. https://github.com/
3. https://about.gitlab.com/
4. https://stackoverflow.com/
5. https://www.iso.org/standard/71278.html
6. https://csrc.nist.gov/publications/detail/sp/1500-4r2/final
7. https://ec.europa.eu/easme/en/news/general-data-protection-regulation-gdpr-now-applicable-are-you-ready-it
8. https://creativecommons.org/licenses/
9. https://www.openaire.eu/research-data-how-to-license/
10. https://www.datprof.com/
11. https://order.shareit.com/product?vendorid=20350&productid=300067878&affiliateid=200286943
12. https://www.red-gate.com/products/sql-development/sql-data-generator/
13. https://www.ca.com/us/products/ca-test-data-manager.html
14. https://zenodo.org/
15. https://openaire.com/?gclid=Cj0KCQjwgMqSBhDCARIsAIIVN1W6VlliodF1H8RHAzH04r1k7W533kdOEfbgw6KgEddic02Jso4b_mEaAsM_EALw_wcB
16. https://www.researchgate.net/
17. https://www.academia.edu/