

United Nations
Global Working Group on Big Data for Official Statistics
Task Team on Access and Partnerships

Deliverable 3: Template for MOUs with global data providers

D R A F T

09/10/2015

This document is based on analyses of current partnership agreements and templates provided by statistical organisations. It provides a list of items that are relevant when engaging into a partnership agreement with data providers and a template of a partnership agreement which can be adjusted to the specific purpose of a partnership between a data provider and a statistical organisation. It makes part of the deliverables of the Task Team on Access and Partnerships (TTAP).

Introduction

Reference to the deliverable

According to its Terms of Reference (TOR), the objectives of the Task Team Access and Partnerships are “to facilitate access to Big Data sources for official statistics and facilitate forming partnerships with other public and private organisations in order to work with Big Data. This should be done in a way that reflects a mutual understanding with partners of what is reasonable to expect from each other, by respecting each other’s position, role, aims, business model, social responsibilities, limitations and possibilities.”

The TOR also states: “Access to Big Data sources and forging partnerships with other public and private organisations in order to work with Big Data is becoming ever more important to national statistical systems (NSS) for fulfilling their mission in society. The NSS should collaborate rather than compete with the private sector, in order to advance the potential of official statistics. At the same time, the NSS should remain impartial and independent, and invest in communicating the advantages of exploiting the wealth of available digital data to the benefit of the people. Building public trust will be the key to success.”

The TOR defines four deliverables. The third one is described as follows:

Templates for memorandums of understanding (MOUs) or service agreements with global data providers, covering the most promising Big Data sources, in particular those already identified by the GWG.

Content of document

In order to compile this document, organisations who had replied positively on the question of already established partnerships in the Big Data Survey in 2014 were contacted for providing anonymised agreements as input to the deliverable 3. In addition, members of the subgroup of the TTAP supplied templates and term sheets for data sharing and license agreements. The documents were analysed and provided input to the current document. During the analysis it became apparent that it will not be possible to provide a ready to use template as the conditions for data access and the nature of projects may vary considerably, thus affecting the type and structure of the agreement. The agreement depends e.g. on the type of project, whether the agreement serves to access data or should constitute a partnership among the contracting parties. The agreement could assure access to data for exploration, prototyping and data production purposes. The agreement could be made between data provider and the statistical office or could include other partners such as data agents or research organisations.

Due to these differences the document first elaborates general items, such as purpose of the agreement or responsibilities of the involved parties and then identifies points to be considered under these items.

Initial Considerations

When engaging into a contractual relationship there are a number of considerations to be made, e.g. among one of the most important is the purpose and scope of the agreement, as these will determine its type and structure. The following text elaborates on a number of considerations.

For simplicity it is assumed that a statistical office would be involved in the agreement. Normally, the statistical office would act as data receiver, and the agreement's object would be to define the terms and conditions according to which the Data Provider will allow the statistical office to access and process certain data (mostly on a noncommercial basis). However, the statistical office can also take other roles, such as data provider or partner for research. In the latter case, the statistical office and the data provider will collaborate in the research and processing of data to reach a jointly defined objective.

Points to be considered

The first consideration would be on **who would be involved in the agreement**. The potential actors very much depend on the type of the agreement, being granting a license to access the data or jointly conducting research on data, a consideration which, in turn, depends on the nature, mission and expertise of the parties. There are examples of data licensing and partnership agreements between NSOs, data providers and universities, or data agents.

After having identified the potential parties, the next step would be to analyse whether a **formal agreement** would be strictly necessary. The legal requirement for an entity to sign a contract may be

triggered by the application of sector-specific legislation or regulation (e.g. Health Insurance Portability and Accountability Act (HIPAA), Safe Harbour, onward transfer agreements, other laws, or upstream contracts), and may depend on the qualification of the data in question as personal data or sensitive personal data. In addition, some companies opt for signing separate agreements: one for the provision of services and another one for contractual allocation of risks, compliance duties, liabilities etc. There are many examples of agreements for data sharing or access. Some jurisdictions provide a template/form that is required to be used and is, therefore, non-negotiable; others create forms that are not amendable but are optional to use. Either way, there is a considerable divergence on how data sharing is approached by various actors. Here are a few specific examples:

- SCC 2010, 2001 (Scalable, free translations, no changes allowed, strict flow down, admin burden, third party beneficiary rights, local firm, jurisdiction, cooperation with authorities, jurisdictional scope limitations)
- National form agreements
- A company's self-drafted agreement, which includes clauses that best suit that company's situation. Section XX of this Deliverable provides certain examples of articles that may be found in such agreements.
- Often, a company's terms and conditions may be stipulated in the form of a "click-through" agreement. Nevertheless, if the company's main agreement (terms of use) is online, the Data Recipient may still request that an independent (and negotiated) agreement be signed between the two parties. In such a case, it is advisable that the negotiated agreement contains a clause that states that this independent agreement overrules the click-through agreement.

The analysis of the requirement for entering into a contractual relation should as well answer the question on the degrees of freedom to negotiate between the potential parties.

The **purpose and aim of the agreement** very much determines its type. Is it a simple one-way data provision or does data flow in either direction with mutual benefits? Are several partners involved in data analysis? Should the agreement serve the purpose for research on the data or should it lead to a regular production of statistical data? Defining the purpose of the agreement should be, as well as the services to be provided by the involved parties.

Other adjacent considerations pertain to the **financial arrangements** of the agreement: In cases where the parties envision a collaborative/partnership framework, it is not unusual that each party bears its own costs under such collaboration, and that sharing of the data is granted at no additional costs or fees. On the contrary, in case where the parties negotiate in a commercial context, access and use of the data might be granted in return of a licensing fee, which could also cover certain additional services to be provided by the data provider.

An agreement should cover the **activities, rights, obligations and responsibilities** of the involved parties. The licensing terms of access to the data as well as the modalities of such access (e.g. providing mobile phone data via a server) should be described, as well as any additional services that are requested from the data provider, . In a data provider / receiver setting, the provision of additional services would mainly apply to the data provider while the data receiver would mainly have to conform and respect the limitations set by the Data Provider regarding the access and use of the data, as well as the communication of the research results. Nonetheless, the data recipient could also be required to perform certain services, especially if access to the data is granted at no fee. The

application of sector-specific legislation may also impose additional requirements on the data recipient with respect to the use of data, including setting up and maintaining safety and security mechanisms for the keeping and processing of such data (these are further discussed below).

The agreement should further define the **relationship between the involved parties** regarding its implementation, and in this context, it should provide for communication and dispute resolution mechanisms arising out of the performance of each party's obligations. Furthermore, in partnership projects where the continuous cooperation between the parties is required throughout the term of the agreement, the agreement should describe how such collaboration will be realized. One possibility could be to set up a steering/consultation committee composed of representatives of the parties to decide on specific items, such as publication and communication of research results, reviewing of work progress or settling disputes at first instance. A steering/consultation committee might also be suitable in partnership agreements with involvement of public entities. The parties should ensure that the agreement clearly sets the responsibilities of such committee as well as its working methods (e.g. composition, decision making processes).

It is important to analyse the **type of data** especially if personal data or confidential data would be exchanged. As a first step, it would be important to identify any personal and confidential data falling under the scope of the agreement. Statistical offices usually already have definitions regarding personal data, however due account should always be taken of the definitions contained in applicable legislation, as, in case of discrepancies, the latter definition would prevail. Any laws that apply to this particular type of information nationally or across the jurisdictions which are covered by the scope of the agreement (or the scope of data processed) should be considered. In general it is recommended to work with non-personal information, public information and information that has been de-identified prior to its disclosure to the data recipient. In this case, it is advisable to include provisions in the contract requiring data providers to ensure that all information will be de-identified prior to its disclosure. In other words, unless access to personal data is unavoidably needed for the project in question, data recipients are advised to require from their partner/data provider to take on the obligation of anonymizing it following their own protocols. This gives comfort to the data providers that they are in control of how the information is being anonymized and reduces their risk of them being held liable for unauthorized sharing of personal data of third parties.. It also gives data recipients the possibility to reduce their own liability by not dealing with personal data, and therefore to reduce the cost for legal compliance that is associated with handling personal data. Usually statistical offices have already long standing experience in working with personal or confidential data and existing rules could be applied to big data sources.

It is important to exactly define the type of data to be accessed as this might be important for statistical analysis. In principle, data should be as less pre-processed as possible or the pre-processing would have to be analysed carefully to assess implications on statistical inference. Data confidentiality might depend on the parties involved and the nature of data. Private parties have other requirements related to confidentiality than research institutes. Quite often businesses already have defined data confidentiality and set up requirements for dealing with confidential data. The agreement should include rules or restrictions related to confidential data during runtime as well as in case of termination or expiration of the agreement.

Some jurisdictions, and subsequently companies, ask for a **data breach notification** to be provided to those who are affected by a breach. This is also a common requirement in case of processing personal

data. Providing a breach notification may have some cost implications. Therefore, asking to include proper clauses in the agreement requiring a breach notification is an important consideration to have.

Confirm if there are appropriate **security and administrative safeguards** in place and whether they are available to you. If there are no existing safeguards, ask if you are the one required to provide them. This will help establish who will be responsible for security breaches/data loss and/or how the security breaches/data loss occurred. Other components of security clauses may require and/or consider the following:

- Physical controls and logical controls (security features, such as sign-on logs)
- Encryption, masking, data anonymisation
- Account access and access controls; passwords
- Network security and intrusion detection
- Data retention, backup and recovery
- Incident response
- Use of subcontractors by cloud provider, data location (if the data is stored in a cloud)
- Security certifications
- Audits

It is also critical to allocate **commercial risks** related to data handling before entering into any type of agreement. Therefore, it is important to understand what risks exist. In this connection, it is recommended to consider the following:

- Data security breach at service provider; notification of data subjects, in cases of breach of personal data;
- Suspicions of data security breach, publicity affects service provider's stock price
- Government inquiries, investigations, litigation discovery
- Customer collected/uploaded data in violation of law; service provider becomes subject to claims
- The above risks could be covered in the clauses requiring partners to be compliant with applicable laws and standards (e.g. obtaining proper licenses, permits, consent for data sharing), or when giving certain warranties, providing disclaimers, or limiting liability.

Normally use of data would be restricted to the purpose defined in the agreement. However, it could be beneficial to include clauses that allow **analysis of data for other purposes**. This would necessitate defining rules on how to communicate and agree on new purposes.

One important topic would be to define **rules on publicizing results** from activities of the partnership. This could be scientific articles in case of research projects or statistics derived from big data sets. These rules should also include agreements of ownership of the results. In the case of research projects it would be important to articulate that publications should not be influenced by predefined objectives but only be based on scientific principles. In addition to ownership of inputs and outputs, it is important to define intellectual property rights that are assigned with the data. The agreement should contain a kind of governance structure, defining at least the points of contacts. In certain cases (e.g. when some form of ongoing collaboration is required between the parties) it might be useful to create a coordination committee and define activities and responsibilities, such as described above.

The agreement should contain the **start date and the duration** of the agreement as well as specifications on when activities would be performed, such as transfer of data. In addition, specifications on prolongation, if considered as useful, and termination of the agreement by either party should be included.

The main part of the agreement should cover the above described items while technical specifications, such as description of data and data format could be put into an annex to the agreement.

Possible structure of an agreement / MoU on data sharing/access

- Identification of parties
- Recitals (aims, activities and purposes of parties)
- Definition of Terms
- Purpose of agreement; (activities of, contribution by, and) relationship between partners/parties
- Data license - conditions for access to and use of data
- Services, Commitments and responsibilities of Parties
- Financial arrangements
- Publicity; communication of results; acknowledgement and use of parties' names
- Communication, consultation and mutual information; (establishment of a coordination committee, in cases of partnership/collaboration agreements)
- Personal information
- Confidential information
- Intellectual property rights
- Entry into force, term, modification, termination of the Agreement
- Resources
- Dispute Resolution
- Warranties, limitation of liability
- Annex: data format, technical description of data access, description of security facilities for data access/transfer, storage

POINTS OF CONSIDERATION FOR AN MOU / AGREEMENT FOR DATA SHARING/ACCESS

The following enumeration mainly contains points relevant in the context of an agreement between parties for access to and sharing of data between statistical offices and other parties. General points such as place of jurisdiction, should be inserted into an agreement but are not discussed in this document.

LEGAL IDENTIFICATION OF THE CONTRACTING PARTIES

Possible signatories:

- Statistical Office (Data Recipient)

- Data Provider
- Intermediate
- Research Organisation

RECITALS

- **Description of the activity** of each Party, leading to the present agreement
 - For a Statistical Office, reference can be made to the legislative framework permitting the SO to engage in the specific activity
 - reference may also be made to any existing big data strategies/initiatives/goals in the context of the Statistical Office's operations
- Description, if necessary, of the actions taken by each prior to the signing of the agreement
-
- Declaration of the mutual intention of the Parties to cooperate on a pro bono or commercial basis within the context of the present agreement and in accordance with its terms and conditions.

Article 1 - Definition of Certain Terms in the Agreement

Commonly defined terms include:

- Agreement
 - e.g. shall mean the present Agreement and any Annexes and Exhibits incorporated herein together with any amendments hereto made in the manner described in this Agreement.
- Data
 - e.g. the data elements listed in the Annex to the Agreement - along with any updates provided from the Data Provider from time to time - which are provided to the Statistical Office by the Data Provider for the purpose and in the context of this Agreement
- Statistics
- Confidential (/ Proprietary) Information
 - e.g. all information disclosed under the Agreement by either party to the other (subject to the exceptions defined in the Agreement), including without limitation all business and product plans, marketing information, and other business information so disclosed; the following shall not constitute Confidential Information: information which (1) is known by the receiving party prior to disclosure by the disclosing party; (2) is or becomes available publicly other than as a result of a breach of this Agreement; (3) is developed independently by the receiving party without the use of or reliance on the disclosing party's Confidential Information; or (4) is provided to the receiving party by a third party under no duty of confidentiality to the disclosing party.

- De-identification
 - e.g. the process of removing, coding, encrypting or otherwise eliminating or concealing the data elements that makes Data individually identifiable to a particular individual, and includes the removal or concealing of any data elements specifically required by law or contractual obligation to be removed or concealed to make Data not individually identifiable to a specific individual or other elements of the Data that are required by law to be de-identified
- Re-identification
- Personal Data
 - e.g. any information relating to an identified or identifiable natural person
- Sensitive Data
 - e.g. any Personal Data pertaining to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and any data concerning health or sex life.
- Intellectual Property Rights
 - e.g. *all copyright, moral rights, patent rights, trade marks, design rights, rights in or relating to databases, rights in or relating to trade secrets and confidential information, rights in relation to domain names, and any other intellectual property rights (registered or unregistered) throughout the world*
- Disclosure
- Permitted Use
 - e.g. shall mean the use of the Data solely for the Project in and accordance with the terms and conditions of this Agreement
 - term may also specifically define how the Data shall be used by the Data Recipient or refer to the corresponding article of the Agreement containing the license grant
- Project
 - description of the Data Recipient's project or activity, within the content of which the Data shall be used
- Project Outputs
 - e.g. *any Project publications, studies, deliverables, products, services and/or technology already developed or being developed by or on behalf of the Data Recipient from time to time which contain data elements of the Data or are based on such data elements, and which are intended for communication or distribution to the public or to third parties*

Article 2 - Purpose of the Agreement, and Relationship between the Parties

- Clearly define the object of the Agreement, its purpose and the nature of relationship between the Parties
 - collaboration between the Parties involving the processing of Data and joint effort to produce a Project Output on a noncommercial basis
 - access to Data on a commercial basis / subject to a payment of an access/license fee
 - access to Data on a noncommercial basis
-
- Include reference to the specific purpose for which Data is shared/accessed
- If requested, a condition can be included that before granting any access to the Data, the corresponding project must be approved in writing by Data Provider

-
- In case of collaboration, reference should be made that such collaboration is on a non-exclusive basis.
- In case of a collaboration, reference should be made that such collaboration cannot result in de facto standardization of Data Provider's goods and services and that there is no advantage in a procurement exercise in the future

Article 3 - Data License

- Grant of License by the Data Provider to the Statistical Office/Data Recipient to use the Data
 - e.g. Subject to the terms and conditions of this Agreement, Data Provider grants Data Recipient, and Data Recipient accepts, a limited, non-exclusive, non-transferable license to use the Data for the Permitted Use (as such use is defined in Article 1) during the Term of the Agreement
 - Depending on whether the Agreement is a commercial agreement or not, the license may be granted in exchange of a license fee (this is mentioned in the article pertaining to financial arrangements)

Article 4 – Services, Commitments and Responsibilities of Parties

- Data Provider may be requested to provide specific services to Data Recipient, or may be burdened with certain additional responsibilities, such as:
 - Provide access to data based on specific queries by Data Receiver
 - e.g. Data Provider shall ensure that Data Recipient acquires and retains access to Data throughout the Term of the Agreement, and shall provide Data Provider with all information necessary to access and use such Data for the purpose of the Permitted Use.
 - Contribute to the actual processing of the Data (in collaboration agreements):
 - e.g. Data Provider shall contribute to the joint work with its methodological and analytical expertise on the use of Data for social and economic analysis.
 - Provide access to de-identified data only, subject to confidentiality, de-identification and aggregation provisions of the Agreement
 -
 - Archive Data for a certain period of time as may be needed for a project and as agreed by the parties
 - Provide access to Data as soon as the general terms of the pilot project are approved, but no later than a specific date
 - The agreement should also define the guaranties, procedure and modalities for Data's disclosure, delivery to and access by Data Recipient. In this context, the Data Provider may be burdened by additional responsibilities, such as:
 - Data should be provided via [VPN; copy on a hard drive]
 - Data shall be de-identified prior to its disclosure
 - Guarantee to never disclose/deliver personal data
 - Data shall never contain content of private communications
- Data Recipient
 - Data Recipient must define queries to access data in a manner defined by Data Provider

- Data Recipient must seek Data Provider’s written permission for every project use for which Data are being used
- Data Recipient must use Data solely for the Permitted Use as described and prescribed in the relevant provision of the Agreement.
- Data Recipient must also respect the conditions and limitations imposed by the Data Provider on the use of Data, which may include the following:
 - not to attempt to re-identify Data de-identified by Data Provider
 - Re-identification may be permitted only with Parties’ mutual agreement and on condition that an individual’s whose data is being re-identified has given its consent
 - to treat the Data as “Confidential Information”, in accordance with the relevant provision of the Agreement, (alternatively, not to communicate, disclose, make available or distribute the Data, or any part thereof, to the public or to third parties, without the Data Provider’s prior written consent)
 - to prevent unauthorized use and disclosure of the Data by taking appropriate security measures including, but not limited to, providing physical security for copies of the Data and taking all steps Data Recipient takes to protect information, data or other tangible and intangible property of its own that Recipient regards as proprietary, confidential or non-public.
 - to notify the Data Provider as soon as it becomes aware of any suspected or threatened infringement by any third party of Data Provider’s rights on the Data.

Article 5 - Publicity, Communication of Project Outputs

- Parties may publicly refer to the existing relationship or this agreement only with the other Party’s prior consent
-
- In cases where the Data is non-confidential and anonymized, the Data Provider could allow the Data Recipient to use it, or part thereof, in the Project Outputs, which, in turn could be publicly disclosed.
 - e.g. When Data is displayed in a Project Output, Recipient will include an attribution notice on that source page acknowledging the Data Provider. The exact wording, format, location and display of any such notice and source page will be at Data Recipient's discretion.
- In cases where the Data is confidential, then the Parties may decide that no publicity should be given to the Project Output.
 - e.g. Data Recipient may not communicate, make available or distribute the Data, or any part thereof, to the public or to third parties. By way of clarification, this restriction extends, but is not limited to, the following actions: a. Altering, modifying, merging or otherwise including the Data, or any part thereof, in any Project Output; b. Copying or reproducing the Data, or any parts thereof, for distribution to the public or to third parties; and c. Selling, transferring, leasing or otherwise assigning the license granted to Data Recipient under this agreement, in whole or in part.
- Alternatively, the Parties might wish to select a procedure for public disclosure of Project Outputs based on Data, which may or may not contain the Data itself, e.g:

- seek Data Provider’s approval before public disclosure of any information (including research publications) that are based on Data
- Parties inform on publications in defined time span before publication date
 - Data Recipient should approve within [a reasonable time - []] and cannot unreasonably withhold approval
- Prohibition of disclosure certain information which the findings are based on (e.g. Data Recipient cannot disclose the following information, unless approved by Data Provider in advance):
 - A geographical specification and/or
 - Specific company/name and/or
 - Country giving rise to Data
- Additional arrangements for the disclosure/non-disclosure of Confidential Data may be provided in the article regarding certain information
 - e.g. Any disclosure or dissemination of the Project Outputs, in any form realized, will respect the rules protecting statistical confidentiality and personal data, specifying that these Project Outputs were achieved in the context of cooperation covered by this Agreement and on the basis of the use of the Data as a source.

Article 6 - Financial Arrangements

- if the agreement is not made on a commercial basis, then it is expected that the Parties will use their own funds or funding sources to implement the agreement, and that there will be no license fee for accessing and processing the Data
 - e.g. Each Party shall use its own funds or funding sources to perform its responsibilities under this Agreement.
- if the agreement is made on a commercial basis, the Agreement needs to contain information on the conditions and modalities for the payment of the license fee.
 - e.g. . In consideration of the License granted pursuant to Article 2 of this Agreement, Data Recipient shall pay Data Provider a license fee of <amount in writing> for the duration of the Term (“License Fee”). The entire License Fee shall be due and payable <number> calendar days after the signing of the Agreement by both Parties. Payment shall be made to the following bank account of the Data Provider: <account details>

Article 7 – Consultation, Committee

- Both parties to appoint focal points for communication regarding any issue relating to the implementation of the Agreement.
 - e.g. Any notices or other communications required under this Agreement shall be deemed sufficient if sent by first class registered airmail to the other party and if addressed as follows:
 - If to Data Provider: <contact details>.
 - If to Data Recipient: <contact details>.
- In cases where the Parties are required to cooperate further for the implementation of the Agreement, it is advisable to provide for a Coordination Committee, as well as to describe its structure (e.g. number of members, appointment of chair), competence (e.g. monitoring the

implementation of the Agreement, decide on any matter not specifically regulated in the Agreement, ensure quality of results, propose/take actions for improving quality and/or resolving disputes, etc.), working methods (e.g. location and frequency of meetings) and decision making processes (unanimity, consensus, voting), including the resolution of potential disputes within the Committee (e.g. recourse to the dispute resolution mechanism provided for in the Agreement).

- e.g. For the implementation of the Agreement the Parties agree to set up a coordination committee (the “Committee”) composed of two representatives of each Party. Within 30 days of signing this Agreement each Party shall notify the other in writing of the names of their representatives on the Committee. It is the faculty of the Parties to proceed with the replacement of their representatives by giving prompt written notice to the other Party. The Chair of the Committee shall be one of the representatives of <designated Party>.

The Committee shall: a. monitor the status of implementation of the activities described in this Agreement; b. identify the measures to be taken to resolve any problems highlighted by the Committee or any of the Parties; c. verify the quality of the results achieved in the performance of activities; and d. proposed any action deemed useful for the enhancement of the results achieved under this Agreement.

The Committee shall meet every semester, or sooner if both Parties agree. Members of the Committee who are not physically present at the location of the meeting may participate through videoconferencing.

The Committee shall decide on all matters by consensus. In case consensus cannot be reached, the Parties shall apply the dispute resolution process of article <number of article>.

Article 8 – Personal Information

- Where Data contains personal information, this article would describe any obligations with respect to such processing; reference to applicable legislation (data protection law, statistical law) may also be made:
 - e.g. The Parties shall ensure that all information exchanged and processed under this Agreement is handled in accordance with all applicable legislation concerning the protection of personal data and statistical confidentiality
- If no Personal Data are contained in the Data, the article could contain a representation by the Data Provider that no personal data are transferred to the Data Recipient in the context of the Agreement
- In case where the Data Recipient receives personal data in the context of the Agreement, the Parties may wish to stipulate additional requirements and, as the case may be, appropriate references to the role of the Privacy Protection Officer

Article 9 - Confidential Information

- This article is largely related to the article dealing with the Publicity and Communication of Results, above. In this sense, the contents of these two articles could be merged or, if the Data is not confidential, the present article may be deleted.
- Definition and types of information that is Confidential:

- Depending on the scope of the Project and the nature of Data, various approaches are possible: All Data (and any derivative information thereof) is and shall be treated as Confidential Information at all times
 - If the Project Outputs contain only the Research Findings and not the Data itself, it may not be considered as Confidential Information.
 - Research Findings mean data analytically derived from Data or other Confidential Information, which have been aggregated and do not disclose Confidential Information nor the Data itself .
 - Information that can be considered confidential in the industry where the Parties operate
- Handling of Confidential Information
 - Parties agree to:
 - Use the same care as it uses with its own Confidential Information
 - Not to disclose Confidential Information other than for the Purpose and to the extent necessary for the Purpose
 - Ensure that employees and representatives who have access to the data are bound by the confidentiality provisions of this Agreement
 - Not to disclose Confidential Information to any third party, unless exceptions apply (as listed below)
 - Prevent unauthorized access to Confidential Information
 - Make sure Confidential Information is not reproduced unless the same proprietary and confidentiality notices and legends as appear on the original Confidential Information remain
 - Accesses only by authorized personnel (*sometimes such personnel may have to be identified and approved by Data Provider)
 - Stored/or accessed only via secure network/computers/hard drives etc. following proper security protocols, identified in a separate Annex []
 - Data shall not be stored outside of/or be only stored within certain geographical location (e.g. with due regard to data localization laws)
- Exceptions for Disclosure of Confidential Information
 - Parties may grant access to the following third parties:
 - Its employees, officials, representatives and agents who have a strict need to know the contents of Confidential Information, and employees, officials, representatives and agents of any legal entity that it controls, controls it, or with which it is under common control, who have a similar need to know the contents of the Confidential Information
 - Any other person or entity with the Data Provider's prior written consent
 - With whom Parties have an agreement, sufficient to require that third party to treat Confidential Information in accordance with this Agreement
 - If such disclosure is required by law
 - Other exceptions for disclosure of Confidential Information
 - is obtained without legal restriction
 - is disclosed by the Data Provider to a third party without any obligation of confidentiality
 - is previously known
 - is at any time developed completely independently of any disclosures hereunder

- Destruction of Confidential Information
 - Parties' obligation to return and destroy all Confidential Information
 - All Confidential Information shall be destroyed upon Data Provider's written request

Article 10 - Intellectual Property rights

- The content of this article could vary considerably, depending on the nature of the Agreement as a partnership agreement on a noncommercial basis, or as a commercial data license agreement. The Parties could decide, inter alia, on the following matters:
- IP rights in materials preceding the Agreement / ownership of the Data:
 - e.g. (for collaboration agreements:) Each Party will own and retain all rights to its pre-existing IP and any IP that is developed outside of the implementation of the Agreement and that is contributed by such Party to the Project Outputs s.
(for one-way licensing agreements:) Data Recipient acknowledges that it has no right or interest in the Data except as expressly provided by this Agreement, that its rights to use the Data are limited to those expressly provided in this Agreement, and that all title and rights to the Data and all data and metadata thereof (including but not limited to intellectual and industrial property rights, neighbouring rights as well as database rights) are vested exclusively in Data Provider
- **IP rights in the Project Outputs/research results:**
 - e.g. Data Recipient will retain all Intellectual Property Rights in all Project Outputs, Recipient Works and all content collected through or used in connection with the Project Outputs (other than the Data)
Data Recipient grants Data Provider a non-exclusive, non-transferable, perpetual, royalty-free, worldwide license to use, display, perform, reproduce, publish, copy and distribute, for[non-commercial purposes] the Project Outputs
 - in cases of collaboration agreements, the Parties could decide to share ownership of the Project Outputs.
 - e.g. Each Party hereto shall jointly own an equal, undivided, one-half (1/2), unrestricted interest in each and in all Project Outputs, and shall notify the other Party with respect to any non-commercial use of such Project Outputs outside the context of the Agreement. The Parties shall agree in advance and in writing on any other potential exploitation of the Project Outputs outside the context of the Agreement.
- Wherever possible, it is suggested that the data created will be published by Statistical Office under a Creative Commons Attribution

Article 11 - Agreement Term, Amendments and Termination

- Effective date, Term, Amendments
 - e.g. This agreement shall enter into force on the date it is signed by the Parties and continue [until terminated / or for <specific duration>]..
No statement or writing subsequent to the date of this agreement purporting to modify, change or add to the terms and conditions here will be binding unless consented to in writing by duly authorized representatives of the Parties in a document making specific references to this Agreement.
- without cause (usually for agreements having an indefinite duration):

- e.g. Either party may terminate this agreement on giving the other at least 90 days' written notice to the other Party
- Termination for cause
 - e.g. This Agreement may be terminated by either Party (the "non-breaching Party") upon written notice of termination in the event that the other party (the "breaching Party") materially fails to perform or observe any material term or provision of this Agreement, and does not cure such breach in all material respects within thirty (30) days following written notice from the non-breaching party demanding the correction of such breach (which notice shall describe such breach in sufficient detail to permit the breaching party to correct such breach). Such termination shall be at no cost for the non-breaching Party.

Data Provider may terminate this Agreement by providing thirty (30) days written notice to the Data Recipient in the event that the Data Recipient makes a general assignment for the benefit of creditors, or files voluntary petition in bankruptcy or files for reorganization or rearrangement under the bankruptcy laws, or if a petition in bankruptcy is filed against the Data Recipient, or if a receiver of trustee is appointed for all or any substantial part of property or assets of the Data Recipient
- Effect of expiration or termination:
 - To existing obligations incurred by the Parties:
 - e.g. Termination of the Agreement pursuant to this Agreement shall be without prejudice to any commitments incurred by the Parties in accordance with the terms of this Agreement, prior to the date of termination. Termination of this Agreement will not affect Data Recipient's right to use any Project Outputs
 - Post-termination obligations - survival of certain terms of the Agreement
 - e.g. Upon the termination or expiration of this Agreement for any reason, Data Recipient's license to use the Data shall terminate and Data Recipient shall immediately cease all use of the Data or metadata thereof. Data Recipient shall within thirty (30) days of the date of termination destroy or return to Data Provider all copies of the Data in its possession or control and shall provide to Data Provider a certification signed by an officer of Data Recipient evidencing such return or destruction. The provisions of Articles [e.g. <article on indemnity>, <article on intellectual property>, <article on publicity and communication of Project Outputs and article on confidentiality>, <article on post-termination obligations>, <article on auditing rights of the Data Provider>, <article on settlement of disputes>] shall survive any termination or expiration of this Agreement.

Article 12 - Resources

- The purpose of this article is that the parties agree on mobilized resources and bearing costs for execution of activities.
 - Each involved party could bear the costs for its activities:
 - e.g. Parties will work in the activities above explained, using each of its facilities and resources;
 - each Party should bear the costs arising from its participation in the activities mentioned in this Agreement.

Article 13 – Dispute Resolution

- Amicable resolution of disputes
 - e.g. The Parties agree to adopt a flexible approach and make reasonable efforts to resolve issues as they arise without recourse to unnecessary escalation.
- As a last resort, arbitration may be set as a dispute resolution process
 - e.g. Any dispute concerning the interpretation or the execution of the present Agreement, which cannot be settled directly between the parties hereto, shall, at the request of either Party, be decided by a sole arbitrator to be nominated by [e.g. the Court of Arbitration of the International Chamber of Commerce]. The arbitration shall be carried out in the English language in <location> in accordance with the Rules of Conciliations and Arbitration of [the International Chamber of Commerce] as then in force. Any arbitration award shall in substance be based on the provision of this Agreement, which shall be interpreted in accordance with <country> law. The arbitration award shall be binding and final, without any recourse to courts or tribunal.

Article 14 - Warranties and limitation of liability; Data Provider's warranties

- e.g. Data Provider warrants that it has and will retain all necessary rights and consents to grant the licences in this Agreement and that the Data does not violate any law or regulation (including data protection legislation) or infringe any third party intellectual property rights. Other than that, Data Provider makes no warranty or representation, express or implied, with respect to the Data and the data contained therein, including, without limitation, its merchantability, fitness for a particular purpose or condition, accuracy, usefulness, completeness or materiality.
- Data Recipient's warranties:
 - e.g. Data Recipient warrants that it shall use the Data only for the Permitted Used and only in accordance with the legislation in force.
- Limitation of Liability:
 - e.g. In no event shall either Party be liable to the other for any indirect, special, incidental, consequential or exemplary damages arising out of or in connection with this Agreement, including but not limited to, loss of profits or business opportunity, whether based on breach of contract, tort (including negligence) or any other theory upon which one Party may seek remedies against the other