Research and Innovation Action

Social Sciences & Humanities Open Cloud

Project Number: 823782 Start Date of Project: 01/01/2019 Duration: 40 months

Deliverable D5.9

Framework and contract for international data use agreements on remote access to confidential data

Dissemination Level	PU
Due Date of Deliverable	30/06/2020 (M18)
Actual Submission Date	12/01/2021
Work Package	WP5 - Innovations in Data Access
Task	Task 5.4 Remote Access to Sensitive Data
Type	Report
Approval Status	Waiting EC approval
Version	V1.0
Number of Pages	p.1 – p.36

Abstract:

This deliverable provides a Template Contract on the Provision of Safe Room Remote Desktop Access and, more generally, a Conceptual Framework for Access to Confidential/Sensitive Data. It will aid and enable future international collaborations on confidential/sensitive data use. It serves as advice through necessary considerations and can be adapted to other institutions planning to facilitate access to their confidential/sensitive microdata via Safe Room Remote Desktop Access.

The information in this document reflects only the author's views and the European Community is not liable for any use that may be made of the information contained therein. The information in this document is provided "as is'' without guarantee or warranty of any kind, express or implied, including but not limited to the fitness of the information for a particular purpose. The User thereof uses the information at his/ her sole risk and liability.

SSHOC, "Social Sciences and Humanities Open Cloud", has received funding from the EU Horizon 2020 Research and Innovation Programme (2014-2020); H2020-INFRAEOSC-04-2018, under the agreement No. 823782

History

Version	Date	Reason	Revised by
0.0	15/02/2020	First draft	Beate Lichtwardt
0.1	14/07/2020	Second draft	Elizabeth Lea Bishop
0.2	16/07/2020	Third draft	Beate Lichtwardt
0.3	20/07/2020	Contribution by external expert	Dana Müller (IAB FDZ)
0.31	21/07/2020	Implementation comments external expert	Beate Lichtwardt
0.32	21/07/2020	Transfer document to SSHOC template, edits	Ann-Kathrin Reinl (GESIS)
0.33	23/07/2020	Final amendments and changes	Beate Lichtwardt and Elizabeth Lea Bishop
0.4	27/07/2020	Internal Review by WP Leader	Johanna Bristle (MPISOC)
0.41	28/07/2020	Implementation comments Internal Review	Beate Lichtwardt
0.42	29/07/2020	Edits	Elizabeth Lea Bishop
0.5	30/07/2020	Final amendments and changes	Beate Lichtwardt and Elizabeth Lea Bishop
0.5	31/07/2020	Submission	Beate Lichtwardt
0.6	31/08/2020	External Review by Freya De Schamphelaere	Freya De Schamphelaere (Social Sciences and Digital Humanities Archive – SODHA, Belgium)
0.7	21/09/2020	Review and restructuring suggestions by Ivana Ilijasic Versic	Ivana Ilijasic Versic (CESSDA ERIC)
0.71	22/10/2020	Implementation comments External Review and restructuring suggestions Ivana Ilijasic Versic	Beate Lichtwardt, Dana Müller and Elizabeth Lea Bishop
0.8	07/12/2020	Restructuring and framework contribution by Matthew Woollard	Matthew Woollard (UKDA)
0.81	10/12/2020	Comments on restructuring from Matthew Woollard	Elizabeth Lea Bishop
0.82	11/12/2020	Comments on and implementation restructuring and framework contribution by Matthew Woollard; further restructuring work and edits of D5.9	Beate Lichtwardt

0.83	13/12/2020	Responding to comments from IV; additional text; accepting changes made in last three minor versions	Matthew Woollard
0.84	14/12/2020	Accepting changes, editing, further restructuring	Beate Lichtwardt
0.9	15/12/2020	Final amendments and changes	Matthew Woollard
1.0	17/12/2020	Further edits, amendments and changes; final version	Beate Lichtwardt

Author List

Organisation	Name	Contact Information
UKDA, University of Essex	Matthew Woollard	matthew@essex.ac.uk
UKDA, University of Essex	Beate Lichtwardt	blicht@essex.ac.uk
GESIS	Elizabeth Lea Bishop	ElizabethLea.Bishop@gesis.org
IAB FDZ (Research Data Centre of the German Federal Employment Agency at the Institute for Employment Research)	Dana Müller	Dana.Müller@iab.de

Executive Summary

The purpose of this report is to provide a template for a contract for international access to confidential microdata. The template is based on an existing contract, and the commentary provides details on the scope and detail of the contract noting considerations for changes within particular local circumstances.

The objective is to provide necessary information for two parties to conclude a contract which provides a legally acceptable method to provide cross-national access to confidential data. The basis is an existing contract between the Research Data Centre of the Federal Employment Agency at the Institute for Employment Research (IAB FDZ), Nuremberg, Germany, and the UK Data Service at the UK Data Archive, University of Essex. It provides an important framework for future data use agreements and serves as a generic template that can easily be adapted to other institutions planning to facilitate access to their sensitive microdata via Safe Room Remote Desktop Access.

The commentary also provides a broad brush introduction to the Five Safes Framework and captures the relationship between the Five Safes Framework and the information security standards and the legislative requirements.

Abbreviations and Acronyms

EOSC	European Open Science Cloud
GDPR	General Data Protection Regulation
GESIS	GESIS Leibniz Institute for the Social Sciences
IAB FDZ	The Research Data Centre (FDZ) of the Federal Employment Agency at the Institute for Employment Research
RDC	Research Data Centre
SRT	Safe Researcher Training
SDC	Statistical Disclosure Control
SODHA	Social Sciences and (Digital) Humanities Archive, Belgium
UKDA	UK Data Archive
UKDS	UK Data Service (Service Provider in the UK – lead by UKDA)

Table of Contents

Introduction

Access conditions to data based on personal information differ on the basis of the level of disclosure (or other) risk of those data. If datasets which are based on personal information are de-identified and fully anonymised and there is no risk of disclosure then these data may, subject to the discretion of the data controller, be made 'openly' accessible, i.e., without restriction to the data user. Data which have not been fully anonymised have a risk of disclosure and consequently should only be made available for research use under specific conditions. In this document we refer to this type of dataset as being confidential. Within the literature the term sensitive is also used, but we find that this understates the case. An individual may be identifiable within a survey dataset on the basis of, say location, age and number of children – but none of these attributes are sensitive in the way in which one's sexual preferences or one's medical history may be.

Within the social science data archiving community there are increasing numbers of datasets containing confidential material available through some form of secure access framework.[1] The framework in use will depend on local circumstances, but the non-prescriptive (i.e., informative) Five Safes Framework (discussed in more detail below) has become the de facto 'standard'. Data service infrastructures exist to provide access to data, including confidential microdata for research purposes.

Providing secure access is concerned with compliance with data and privacy protection regulations. Confidential microdata, understood as information that can potentially be used to identify an individual or data subject, must be strictly regulated and controlled.

A secure method of accessing such data is via a secure remote desktop connection accessed through a Safe Room. This approach offers a secure environment to access the confidential microdata. Datasets remain on the secure servers of the data provider (in location A), which are then accessed through a secure encrypted internet connection (from location B). No physical transfer of the confidential/sensitive microdata ever occurs: all browsing and analysis of data are undertaken remotely from location B, on the secure servers that are based in location A. The Safe Room provides additional physical controls (e.g. control of Safe Room access and monitoring by Safe Room staff). Essentially, the Safe Room can be thought of as a physical secured room to protect the access device.

Providing secure remote desktop access to confidential microdata via a Safe Room is a challenge even within one country. Across countries, this poses an even bigger task with many additional hurdles to overcome.

To improve the international research infrastructure and, thus, aid researchers requiring access to international confidential/sensitive microdata to access these data from within their country and without the need to travel abroad, this report provides a Conceptual Framework and Template Contract for international data use agreements on remote access to confidential data between institutions being located in different countries.

[1] See for an example of the approach used by NORC and NIST in the United States: Julia Lane and Stephanie Shipp, 'Using a Remote Access Data Enclave for Data Dissemination', *International Journal of Digital Curation*, 2.1 (2007). https://doi.org/10.2218/ijdc.v2i1.20 [17/12/2020]

The Template Contract is based on an existing contract between the Research Data Centre of the Federal Employment Agency at the Institute for Employment Research (IAB FDZ), Nuremberg, Germany, and the UK Data Service at the UK Data Archive, University of Essex. It is intended to provide a generic template that can be adapted to other institutions planning to facilitate access to their confidential/sensitive microdata via Safe Room Remote Desktop Access. Variations of this contract are in use for multiple access points across Europe and worldwide, proving the value of this template.

It is important to note that the Template Contract needs to be adapted according to the varying legal, institutional and technical requirements of both parties involved, which can differ considerably between institutions and countries. Even the terminology might need to be amended. It is for these reasons that we recommend using unilateral agreements. Finally, the validity of the agreement must always be checked by legal experts of both parties involved and the wording changed, if and where needed.

The Agreement Template Contract includes definitions of terms used in the contract, services of parties outlining the tasks and responsibilities of Party A and Party B, the period of the agreement and options for modification and termination, as well as specifications regarding available research data and the occurrence of fees. Seven appendices add further information on Safe Room Remote Desktop Services in general, the application process for Users, available research data, details on fees, relevant legislative texts, a pledge on data secrecy/ a Secure Access Agreement, and the responsibilities within the hosting institution[2].

[2] For purposes of translation or appropriation of the document with regards to national and other legal terminology, in this document the terms *agreement* and *contract* are used, contract being an agreement between parties creating mutual obligations enforceable by law. Contract contains all the basic elements required for the agreement to be legally binding.

Framework for Access to Confidential Data

Conceptual Framework for Access to Confidential Data

All access to personal data is managed at a national level through legislation; and at a European level by the General Data Protection Regulation (GDPR).

The 'Five Safes' Framework,[3] pioneered by the UK's Office for National Statistics and implemented as part of the UK Data Service's Secure Lab system provides a conceptual basis for the implementation of risk management against the disclosure of personal data and thus the maintenance of the confidentiality of that type of data.

For international collaborations on accessing controlled data across borders an additional concept, that of *equivalence,* is needed to deal with some of the differences between the national implementations of data protection. There is no guarantee that our implementation of equivalence will be valid in any bilateral agreement between a data controller and a data service provider. However, the conceptual agreement works in principle between the UK and Germany, and between Germany and the UK.

Access facilities (Research Data Centres, Secure Labs, Safe Data Havens, etc.) exist to provide secure access to confidential data (usually, but not exclusively, microdata) for research purposes. Providing secure access to confidential microdata is predicated on compliance with data and privacy protection regulations, and the implementation of best practices to minimise the disclosure risk. These data are typified as information which could be used to identify (legal) individuals/data subjects (persons or institutions).

There are different methods of protecting confidential data so that they can be used for research purposes while mitigating the risk of disclosure of personal information. Here we consider using international secure remote desktop access via a Safe Room. This approach offers a safe environment to access the confidential data. Datasets remain on the secure servers of the data provider (in location A), which are then accessed via a secure encrypted internet connection (from location B). No physical transfer of the confidential data ever occurs. All browsing and analysis of data are undertaken remotely from location B, on the secure servers which are based at location A. The Safe Room at location B provides additional physical controls (e.g., control of Safe Room access and monitoring by Safe Room staff). This element of the 'safe environment' element of the Five Safes framework can be made more or less 'safe' by the inclusion of additional controls (which may be a deterrent or a control for monitoring (or both).)

To improve the international research infrastructure and, thus, aid researchers requiring access to international confidential microdata to be able to access these data within their countries, without travelling abroad, we

[3] See: Tanvi Desai, Felix Ritchie and Richard Welpton, 'Five Safes: designing data access for research', University of the West of England, Economics Working Paper Series, 1601. (2016). Available at: https://www2.uwe.ac.uk/faculties/BBS/Documents/1601.pdf [17/12/2020]

provide a Template Contract between two parties, whereby each party represents a mature data service with its own Research Data Centre (RDC) in a different country. This Template Contract is based on an existing contract between the RDC of the Federal Employment Agency at the Institute of Employment Research (IAB FDZ), Nuremberg, Germany and the UK Data Service at the UK Data Archive, University of Essex. It provides a template for future research agreements and can be adapted to other institutions planning to facilitate access to their confidential microdata via Safe Room Remote Desktop Access. Variations of this contract are in use for multiple access points across Europe and worldwide, proving the value of this contract.

Four important areas to note:

1. This contract is predicated on mature (or at the very least) existing 'secure access' arrangements at both parties.
2. The contract will need to be adapted accordingly to the varying legal, institutional and technical requirements of both parties, which can differ considerably between institutions and countries.
3. The contract may also need to alter some specific terminology to make it more appropriate for local requirements.
4. This contract is in English, but it could be translated.

For these reasons, we recommend the use of unilateral agreements~~.~~

Almost all the clauses within the contract relate explicitly or implicitly to the Five Safes Framework. The following paragraphs explain each of the Five Safes in a short definition. This is followed by all of the relevant references within the contract, i.e., those which deal with the specific issue. It should be clear that just having a contract in place does not mean that these elements of the framework are dealt with. Specific documented procedures for each of the parties to the contract may also need to be place.

Also, in these paragraphs, the contract is referenced to a specific clause. S1/S2 refers to Section 1 and Section 2 respectively. PA/PB refers to those parts of Section 2 which specifically refer to the responsibilities of Parties A and B respectively. Any subsections are referred to after the paragraph symbol, i.e., S1 § 6 refers to Section 1 paragraph 6.

The paragraphs below do not refer to contractual matters which are unrelated to the Five Safes Framework.

Safe Data

Data is treated to protect any confidentiality concerns.

S1 § 6 states that Party A "will provide factually anonymised data…" An unnumbered paragraph below S1 § 7 clarifies that the responsibility for the provision of these factually anonymised data is at the sole discretion of Party A. In the event of a breach the responsibility lies solely in the hands of Party A (who may in turn have indemnification from the original data controller, but that again is in the hands of Party A.)

Section 2 heading refers to the data as "factually anonymised." (See also Appendix C)

Safe Projects

Research projects are approved by data owners for the public good.

See S2 PA 2 §3.1 – project end date is known.

Appendix B covers the application process and the fact that projects are reviewed for disclosure risk, feasibility, and "requirement for non-public data." It also covers "public interest and public good" rationale.

The contract does not explicitly say who assesses and approves projects.[4] The rationale here is that different organisations/countries may have different rules. The bottom line is that all projects must be approved according to the rules set down by the data controller, which must be in line with European and local law. In cases where GDPR applies, the project must be in the public interest and for the public good. But data controllers may apply other conditions beyond these two. It is essentially the responsibility for Party A to ensure that the conditions are met for each project, and that the researchers do not extend the remit of their project beyond the approved project application.

Safe People

Researchers are trained and authorised to use data safely.

Full identification of researchers is required in order to correctly identify any individual involved in a breach. In PA 2 § 3.1 users must be identifiable by name and institution (see also Appendix B heading 3). In PA 2 § 3.3 accredited users are given personalised user credentials which also provides the method for ensuring that only a person accredited (through Safe Researcher Training (SRT) followed by an SRT test) is accepted as a user.

Pre-access basic training in safe data handling is a requirement for users. This is covered in PA 2 §7.1 and ongoing support is covered in PA 2 § 5.1.

Safe Settings

A Secure Lab environment prevents unauthorised use and access to the data.

The primary means of implementing of Safe Settings is the provision of a Secure Remote Connection between Party A and Party B (PA § 1.1), and the provision of a 'Safe Room' in Party B (PA Section 2 introductory paragraph and defined in PB Section 1: Safe Room). PA Section 3.3 refers to the significance of user credentials and user project areas. The contract does not mention whether user areas are separate, as this will depend on the

[4] Appendix B says that research proposals will be evaluated by Party A, but this is usually an inspection in advance of the proposal being submitted to a Data Access Committee responsible to the specific data owner.

permissions from the data controller in research project applications. Best practice would ensure that issued user credentials differ for different projects.

Paragraph PA Section 2.8 describes the issue of the maintenance of thin clients and software.

Safe Outputs

Safe outputs are those which have been screened and approved as non-disclosive. No person or organization can be identifiable from the results of an analysis of survey or administrative data.

Under PA § 6.1 Statistical Disclosure Control (SDC) is undertaken by Party A. The specific SDC method is not specified.[5] The understanding is that Party A applies their own method of disclosure control. They are the data processors, so have this responsibility to ensure that the outputs are correctly reviewed to prevent a breach of personal information.

There is also an expectation that the researcher understands enough about disclosure control to not request outputs that are obviously in breach of the rules of Party A's disclosure control. (See also PA § 5.1)

Note that PA 2 § 7.1, while not explicit, assumes that Party A has supplied to Party B the relevant information relating to data security matters and this includes Statistical Disclosure Control methodologies.

Basic training in safe outputs should be part of the training requirement for users. This is covered in PA 2 §7.1.

Legislative Framework

All countries of the European Union have the EU data protection basic regulation in common. But, country-specific laws can also play a role here. Thus, not only EU law but also national law applies to the implementation of data access. It depends on the data itself which national law is applicable. For example, social security data in Germany is subject to the Social Security Code or federal statistics are subject to the Federal Statistics Act. This means that for the implementation of secure data access to confidential/sensitive data, the respective national legislation must be taken into account. The legal departments must decide whether it is necessary to embed national laws in the agreement or not. For the IAB FDZ the following legislation has been taken into account:

- Section 78 German Social Code, Book X (https://www.sozialgesetzbuch-sgb.de/sgbx/78.html),

[5] We recommend the Statistical Disclosure Control Handbook (2019) produced by the Safe Data Access Professionals. Available at: https://securedatagroup.org/sdc-handbook/ .

- Section 282 para.7 German Social Code, Book III (https://www.sozialgesetzbuch-sgb.de/sgbiii/282.html),
- Section35 German Social Code, Book I (according to section 53 of the Federal Data Protection Act) (https://www.sozialgesetzbuch-sgb.de/sgbi/35.html),
- General Data Protection Regulation GDPR (https://gdpr-info.eu/).

Other legislation that might need to be considered by German institutions are, for example:

- Datenschutz-Grundverordnung (DSGVO),
- Bundesdatenschutzgesetz (BDSG),
- Landesdatenschutzgesetze,
- Bundesstatistikgesetz,
- Telemediengesetz (TMG),
- Telekommunikationsgesetz (TKG),
- Datenschutzrichtlinie für elektronische Kommunikation (Richtlinie 2002/58/EG), besser bekannt als ePrivacy-Richtlinie.

For the United Kingdom, as for Germany, national legislation as well as EU legislation play a role, namely the

- Statistics and Registration Service Act, 2007 (Statistics and Registration Service Act, 2007),
- Digital Economy Act, 2017 (Digital Economy Act, 2017),
- Data Protection Act, 2018 (Data Protection Act, 2018),
- General Data Protection Regulation (General Data Protection Regulation (GDPR).

Compliance with data and privacy protection regulations (GDPR)

Compliance with national data and privacy protection regulations is a requirement for any national service provider. Without such compliance the data service would be operating illegally and would be subject to any relevant penalties.

Contract for international data use agreements on remote access to confidential data

This part contains a Template Contract that regulates remote access to factually anonymous research data involving two parties. Party A is responsible for storing the research data, while Party B is responsible for securing the access point to the research data.

As noted above, this contract relates to the specific procedures which are in place in the IAB and the UK Data Archive. Both these organisations have mature (i.e., long running, successful and growing) systems in place for providing remote access to confidential microdata to researchers. Organisations with less mature systems might consider gaining experience nationally before moving on to international data access.

A secured remote desktop connection allows researchers to work via a Thin Client (access device), that is located in a Safe Room at Party B; with the research data stored on Party A servers. The dataset never leaves the facilities of Party A; only screen updates are transmitted to the Thin Client in the Safe Room hosted by Party B (a more detailed description can be found in Appendix A).

The Safe Room hosted by Party B is open to all approved Users of Party A (a detailed description of the application process can be found in Appendix B). Party B guarantees to provide equal and non-discriminative access to the Safe Room to all approved Users of Party A, especially not to over-privileged Users affiliated with Party B.

This contract fixes the responsibilities of Party A and Party B in order to ensure secure access to the factually anonymous research data of Party A. Additional documents (e.g. a non-technical overview of this type of data access system) can be found in the Appendix of this contract.

In the Template Contract there are a number of clauses which *may* need to be considered in light of local practices and procedures. These are marked with an asterisk. More general considerations are discussed in the following section, following the structure of the Template Contract.

Considerations

This section contains a brief summary of what we believe needs to be considered when setting up a contract for international data use agreements on the Provision of Safe Room Remote Desktop Access to confidential data. The full details can be found in the Template Contract. Not all sections require detailed commentary, some have been left to stand for themselves.

DEFINITIONS

Section 1 of the Template Contract includes all definitions. These serve as an example and may need to be amended, changed, or extended for any version of this agreement. For our purposes we have defined the terms User; Secure Remote Desktop Access; Safe Room; Workspace; Thin Client; Research Data; and Period of Agreement and Modification/Termination.

We particularly note the use of the term *research data* which is used to clarify that research is the principal use of the data. This is not a legal requirement but a public perception issue – it is expected that this unambiguously identifies one of the rationale for the existence of these data – they were constructed with research as one of their primary uses. In the body of the contract, we use *data* alone, and it may be found convenient to use this term throughout the contract when reused.

Furthermore, within the contract the term user is used. In most of the document this means a potential user, though it also can mean an 'approved' user. The specific state of a user is dependent on context, and approved will mean approved too access the data by whatever means are locally appropriate. A user which is not approved will not gain access to the systems, so in almost all cases the term user can only mean one who is approved to use the system. In most cases approval means, being accredited by a relevant organisation, having attended relevant training, and agreeing some form of agreement. The term user never applies to data service staff, who will need to be approved locally.

SERVICES OF PARTIES

S2 lists the tasks agreed to enable secured Safe Room Remote Desktop Access to Party A's factually anonymous research data from a Party B's Safe Room. The tasks listed serve as an example and may need to be amended, changed, and extended for any version of this contract.

For both parties separately, we have specified tasks regarding setup/installation; application (user); account (user); access control/monitoring (Safe Room); support; Statistical Disclosure Control; training; maintenance; and Safe Room security.

In the section relating to Party B's responsibilities to monitor users it is not explicit that they have the responsibility to remove and deny access a user, if they are found to be behaving incorrectly. This is implicit inasmuch as should be part of internal monitoring procedures. In the same section no time frame is explicitly mentioned for the period in which Party B should inform Party A of any breach (of information security or procedure). This is expected to be done immediately, but a specified period could be mentioned here, e.g., five working days.

PERIOD OF AGREEMENT AND MODIFICATION/TERMINATION

S3 of the contract has a relatively harsh termination clause: "If terms of the contract are violated the remote connection can be terminated immediately." Two points to note: first, the use of the word 'can' does not mean that it must be terminated, thus Party A may protect the data they have responsibility for in the strongest way possible. Second, if this is felt too harsh, the two parties might enter into mediation. However, if must be remembered that the relevant data controllers might expect this rapid termination of the remote connection to be a default position.

AVAILABLE RESEARCH DATA AND FEES

S4 refers to available research data and fees. If the list of potentially available data is small and unlikely to change over time it could be described here. However, if the list of available research data changed over time (and that is usually the case), then it is easier to simply update Appendix C instead of having to change the main contract and sign it again. Similarly, the reason for 'outsourcing' the details regarding fees into an Appendix is the same, i.e., if they are likely to change, being in an Appendix it can be updated without having to re-execute the contract.

The reason for 'outsourcing' the details regarding fees into an Appendix is the same as mentioned above.

CONTENT OF APPENDIX

This section lists appendices containing further details of the agreement. The details could be included in other parts of the contract. However, as the Template Contract is based on an active contract, its structure, which consists if a main part and appendices, is kept here. The reason for this division into a main body and appendices is that only parts of the agreement need to be amended when updates occur, in this case the appendices. If, for example, the name of the contact person who must sign an obligation to maintain data secrecy (Appendix F) changes, only Appendix F will have to be updated. If this appendix was integrated in the main part of the agreement, the entire agreement would have to be signed again. The same applies to all other appendices. Laws can change over time, the application process changes, as does the list of available research data, the specifications for the remote access etc. etc.. All must be mentioned in the contract, in this case section 5, otherwise it will not be taken into account by the contractual partners.

However, this Template Contract serves as an example and needs to be amended, changed, and extended, or sections deleted as and how it is needed for the particular agreement.

GENERAL DESCRIPTION OF SAFE ROOM DESKTOP SERVICES

A secure method of accessing confidential microdata for research purposes is via a secure remote desktop connection accessed through a Safe Room. This approach offers a secure environment to access the confidential microdata. Datasets remain on the secure servers of the data provider (in location A), which are then accessed through a secure encrypted internet connection (from location B). Only screen updates, mouse and keyboard changes are transferred through the encrypted internet connection. Therefore, no physical transfer of the confidential/sensitive dataset ever occurs: all browsing and analysis of data are undertaken remotely from location B, on the secure servers that are based in location A.

The Safe Room provides additional physical controls (e.g. control of Safe Room access and monitoring by Safe Room staff). Essentially, the Safe Room can be thought of as a physical secured room to protect the access device.

The setting described above requires the collaboration of a minimum of two partner institutions. Party A assumes responsibility for the research data and Party B assumes responsibility for the access point. Responsibilities, tasks and workflows required are fixed in this contract. In addition, knowledge about the other partner and trust in each other’s operating procedures are required.

The research data resides and remains in the location of Party A, and a contract has to be agreed and signed between Party A and the User. Party B agrees to monitor the Safe Room setting and fulfils the required arrangements for permitting Users to access the data, for which a contract is required between Party A and Party B.

APPLICATION PROCESS

The application process differs between institutions and cannot be generalised. The wording serves as an example only. In practice the application process should only collect information which is relevant to decision-making in the application process. For example, a question on the age of a researcher is likely to be irrelevant. However, some information being captured may be used for management information of the service.

Appendix B contains comments on 3 important operating procedures to be followed in administering research projects for access to Party A data. These include a) Applying for data access, b) Application procedure, and c) Formal project agreements.

Confidential data access requires specific procedures in order to control and monitor access and reduce the risk of disclosure. These procedures are designed to ensure that projects meet the goals of both participating institutions. The universal basics include knowing the names (and institutions) of the researchers applying for access to the data --- this is required in order to maintain an audit of each person being allowed to use the data --- and would be used in the case of a breach to identify the people who may the cause of such a breach. The institution of the user is required to apply sanctions to a researcher who breaches the local rules. Some data controllers specifically exclude use outside their country, so the country in which the researcher is based is also collected.

Potential users of data should submit their applications for data access to their national data service provider. Note that these applications may differ depending on the requirements of the data service provider and on the requirements of the data owner. As noted above, while some of the requirements are based on law, they may differ based on the specific risk appetite of the data controller. In general, however, applications should allow those making the authorisation decisions to understand that proposed research actually requires these data; that the research is feasible; and that the proposed research meets any national public interest/public good test which may be required.

Note that the data provider is not necessarily the data owner, and the data owner/controller is responsible for ensuring that the correct procedures are in place for their data to be accessed via a data service. Data services will attempt to have as few different processes as possible to maintain a uniform process for researchers using data from multiple data owners, and also to streamline their internal systems.

Available Research Data

The factually anonymous data will be provided on a project-specific basis. The determination of whether research data are factually anonymous is at the sole discretion of Party A.

Fees

Appendix D specifies the fees for the technical access provision only. Institution specific research project fees or else are not covered by this section, they will be part of the individual access agreement with the user and do not form part of the contract. In general data services are funded to provide this type of access and provide a free-at-the-point-of-use service.

Relevant Legislative Texts

Appendix E lists the documents relevant to the legislative framework of the contract. It contains two sections, one on Country and EU Legislation, and one on internal process/procedure documents.

Pledge on Data Secrecy

The Declaration in Appendix F provides the text that prospective users must fulfil prior to being able to access data. Declaration must be signed by the user and their organisation, and returned before the user can receive access credentials: username and password. The Declaration demonstrates that the prospective User and their organisation understand the seriousness of the undertaking, and that they each understand the penalties that may be imposed for non-compliances with security or confidentiality.

The Declaration is to be agreed and signed by the applicant, who will be the researcher requiring access to the information for his/her own research needs, and by an appropriate officer (in the Research & Contracts Office, or equivalent) from the organisation where they are based.

Responsibility within Party B

Appendix G specifies where responsibility lies within Party B for the tasks specified in Section 2:

Administrative and IT staff will support the following tasks of Setup/Installation and Maintenance specified in Section 2.

The operation of the Safe Room, in particular the tasks of Access control/monitoring of the Safe Room, Support and Maintenance specified in Section 2 will be carried out by staff of Party B.

Template Contract on the Provision of Safe Room Remote Desktop Access[6]

Agreement

between

[Name and address of Party A]

Represented by […]

- hereinafter Party A -

and

[Name and address of Party B]

Represented by […]

- hereinafter Party B -

hereinafter referred to collectively as the Parties

about the

Provision of Safe Room Remote Desktop Access

[6] This Template Contract is based on an existing contract between the Research Data Centre of the Federal Employment Agency at the Institute for Employment Research (IAB FDZ), Nuremberg, Germany, and the UK Data Service at the UK Data Archive, University of Essex.

TABLE OF CONTENTS

INTRODUCTION:

This document contains an agreement that regulates remote access to factually anonymous research data involving two parties. Party A is responsible for storing the data, while Party B is responsible for securing the access point.

A secured remote desktop connection allows researchers to work via a Thin Client (access device), that is located in a Safe Room at Party B; with the research data stored on Party A servers. The dataset never leaves the facilities of Party A; only screen updates are transmitted to the Thin Client in the Safe Room hosted by Party B (a more detailed description can be found in Appendix A).

The Safe Room hosted by Party B is open to all approved Users of Party A (a detailed description of the application process can be found in Appendix B). Party B guarantees to provide equal and non-discriminative access to the Safe Room to all approved Users of Party A, especially not to over-privileged Users affiliated with Party B.

This agreement fixes the responsibilities of Party A and Party B in order to ensure secure access to the factually anonymous research data of Party A. Additional documents (e.g. a non-technical overview of this type of data access system) can be found in the Appendix of this agreement.

THE AGREEMENT

It is hereby agreed between the parties:

*Section 1: Definitions[7]

(1) User

Researcher with a valid contract to work with Party A research data; accessing Party A research data from within a Party B Safe Room.

(2) Secure Remote Desktop Access

Secured encrypted Remote Desktop Connection to a data-processing system held at Party A from an access device at a remote location at Party B. Only mouse and keyboard changes are transferred from B to A and only screen updates are transferred from A to B. The dataset stays at the servers of Party A.

(3) Safe Room

A secured room belonging to Party B used for providing access to confidential/sensitive research data of Party A. Entry is restricted and the setting is regularly monitored by Party B staff. The room is only provided with the access device(s) required to enable Secure Remote Desktop Connections to the distant servers. Only authorised staff from Party B and Users are permitted to access the Safe Room.

(4) Workspace

The workspace is a desk in the Safe Room where a Thin Client is placed. The workspace is protected (i.e. by a partition) and the screen of the access device must not be easily observed by other Users or unauthorised people.

(5) Thin Client

A Thin Client works as access device. It is a computer terminal which only provides an interface (via keyboard, mouse, screen) to the User, and is configured to enable access only to the server of Party A where the data reside (the User will not be able to use the device to access anything else). All operations are carried out on the servers of Party A.

[7] Asterisks preceding a heading means one should refer to the comments in the section Considerations.

(6) Research Data

Party A will provide factually anonymous data that can be accessed on-site via the Party B Safe Room. The factually anonymous data accessible via the Party B Safe Room will be prepared by Party A on a project-specific basis.

(7) Period of Agreement and Modification/Termination

This agreement will become effective when signed by both Parties. Either Party has the option to terminate the agreement upon thirty (30) days advance written notice to the other. If terms of the contract are violated, the remote connection can be terminated immediately. Changes and amendments to this agreement shall be valid only if made in writing and agreed by both Parties.

The determination of whether research data are factually anonymous is at the sole discretion of Party A. Party B and their employees refrain from any kind of interference in this matter.

*Section 2: Services of Parties

Party A and Party B agree to undertake tasks to enable secured Safe Room Remote Desktop Access to Party A's factually anonymous research data from a Party B Safe Room. The responsibilities are structured by topics, if a topic contains no tasks for the given Party, this is stated by the term "none". The tasks are described in the following.

Party A

1. Setup/Installation

    1.1 Party B shall enable a Secure Remote Desktop Connection to designated servers located at Party A.

2. Application (User)

    2.1. All tasks concerning User applications to access Party A data are undertaken by Party A. A definition of the selection process can be found in the Appendix.

3. Account (User)

    3.1. Party A shall inform Party B on a regular basis of entitled Users, including names and institutions of the Users as well as end dates of projects. This information is required for access control.

    3.2. Party A shall provide Party B staff with an authentication code in order to establish the Secure Remote Desktop Connection to Party A servers. This authentication must be kept confidential by Party B staff and must not be shared with anyone, including the data User.

3.3. Party A shall provide each accredited User with personalized User credentials in order to access the data stored in a project area on the servers of Party A. This authentication must be kept confidential by the data User and must not be shared with anyone, including Party B staff.

4. Access Control/Monitoring (Safe Room)

4.1. [None.]

5. Support

5.1. Party A will take responsibility for matters concerning User Support regarding research data, data documentation, application and information about Statistical Disclosure Control issues.

6. Statistical Disclosure Control

6.1. Dissemination of output files and Statistical Disclosure Control tasks (input and output control) will be undertaken by Party A.

7. Training

7.1. Party A will provide information to Party B staff regarding data security issues of Party A data, workflows, organisational structure and all relevant operational instructions.

8. Maintenance

8.1. Maintenance and technical service of the Thin Clients, including software, and the repair of the Thin Clients, will be undertaken by Party B or by contractors instructed by Party B as necessary.

9. Safe Room Security

9.1. [None.]

Party B

1. Setup/Installation (see also Appendix G)
    1.1. Party B will provide a Workspace in a Safe Room.
    1.2. Party B will provide a network point for connecting to the internet in the Safe Room, thus allowing a Secure Remote Desktop Access Connection between the Thin Client and the server hosted by Party A.
    1.3. Party B staff will assist with the establishment of the Safe Room setting (regarding physical security and establishing the Secure Remote Desktop Access Connection to Party A).

2. Application (User)
    2.1. [None.]

3. Account (User)
    3.1. [None.]

4. Access Control/Monitoring (Safe Room; see also Appendix G)
    4.1. Party B will schedule on-site visits to the Safe Room location at Party B for the User.
    4.2. Access to the Safe Room hosted by Party B is open to all Users. Party B guarantees to provide equal and non-discriminative access to the Safe Room to all approved Users, especially not to over-privileged Users affiliated with Party B.
    4.3. Party B staff will verify the identity of Users accredited by Party A upon arrival at the Safe Room.
    4.4. Party B will ensure that only Party A accredited Users have access to the designated Party A workspace.
    4.5. Party B staff will be provided with an authentication code in order to establish the Secure Remote Desktop Connection to the Party A servers. This authentication must be kept confidential by Party B staff and must not be shared with anyone, including the data User.
    4.6. Party B staff will monitor the User(s) to ensure that no attempts to re-identify any confidential or personal information in the provided research data set are made. This

includes e.g.: taking pictures, sharing information with unauthorised persons, use of communication equipment, manipulating hardware and software.

4.7. Party B shall notify Party A of security incidents regarding data privacy and data security.

5. Support

5.1. Party B staff will serve as a local contact for researchers interested in conducting research with Party A data at the Safe Room of Party B.

6. Statistical Disclosure Control

6.1. [None.]

7. Training

7.1. [None.]

8. Maintenance

8.1. Party B staff will assist Party A with the maintenance of the Secure Remote Desktop Connection between the Access Device (Thin Client) and the Party A servers.

8.2. Party B will inform Party A of any technical problems that may occur.

9. Safe Room Security

9.1. Access to the data is permissible as per local laws or protocols of the country in which Party A resides.

9.2. Party B staff in charge with the operation of the Safe Room have to be informed about applicable laws and procedures. More information is provided in the Appendix (E).

9.3. A Secure Access Agreement is provided in Appendix (F). Party B staff involved in Secure Room Remote Desktop tasks must ensure that they are aware of the regulations regarding access to Party A data.

9.4. Party B permits employees of Party A to audit (visit and see) the activities in the Safe Room at any time, provided reasonable notice is given to Party B.

Section 3: Period of Agreement and Modification/Termination

This agreement will become effective when signed by both Parties. Either Party has the option to terminate the agreement upon thirty (30) days advance written notice to the other. If terms of the contract are violated the remote connection can be terminated immediately. Changes and amendments to this agreement shall be valid only if made in writing and agreed by both Parties.

* Section 4: Available Research Data and Fees

The research data from Party A, made available from Party B Safe Room, are described in the Appendix C.

Any fees that arise are laid down in the Appendix D.

* Section 5: Content of Appendix

A. General Description of Safe Room Remote Desktop Services
B. Application Process
C. Available Research Data
D. Fees
E. Relevant Legislative Texts
F. Pledge on Data Secrecy/ Secure Access Agreement
G. Responsibility within Party B

Authorised Signatories:

For Party A ([Signatory, Name Party A]):

__________________________________ Date: ______________

For Party B ([Signatory, Name Party B]):

__________________________________ Date: ______________

THIS CONCLUDES THE AGREEMENT BETWEEN THE PARTIES

APPENDIX A: General Description of Safe Room Remote Desktop Services

Access facilities (Research Data Centres, Population Centres etc.) exist to provide secure access to confidential microdata for research purposes. Providing secure access is concerned with compliance of data and privacy protection regulations. Confidential microdata about individuals (persons, households, institutions), understood as information that can potentially be used to identify an individual, must be strictly regulated and controlled.

A secure method of accessing such data is via a secure remote desktop connection accessed through a Safe Room. This approach offers a secure environment to access the confidential microdata. Datasets remain on the secure servers of the data provider (in location A), which are then accessed through a secure encrypted internet connection (from location B). Only screen updates, mouse and keyboard changes are transferred through the encrypted internet connection. Therefore no physical transfer of the confidential/sensitive dataset ever occurs: all browsing and analysis of data are undertaken remotely from location B, on the secure servers that are based in location A.

The Safe Room provides additional physical controls (e.g. control of Safe Room access and monitoring by Safe Room staff). Essentially, the Safe Room can be thought of as a physical secured room to protect the access device.

The setting described above requires the collaboration of a minimum of two partners. Party A assumes responsibility for the research data and Party B assumes responsibility for the access point. Responsibilities, tasks and workflows required are fixed in this contract. In addition, knowledge about the other partner and trust in each other's operating procedures are required.

The research data resides and remains in the location of Party A, and a contract has to be agreed and signed between Party A and the User. Party B agrees to monitor the Safe Room setting and fulfils the required arrangements for permitting Users to access the data, for which a contract is required between Party A and Party B.

*APPENDIX B: Application Process

The following are important operating procedures to be followed in administering research projects for access to Party A data. These procedures are designed to ensure that projects meet the goals of Party A and Party B.

1. *Applying for Data Access.* Potential Users of data submit their applications for data access to [Name of Party A]. All Users of data shall submit an application for data access.

2. *Application Procedure*. In order to review and approve an application for data access to Party A data the following procedures apply:

The applications will be evaluated by Party A and projects reviewed for disclosure risk, feasibility and the requirement for non-public data. The application must explicitly explain why the research project is for public interest and public good.

3. *Formal Project Agreements.* After the application has been approved by Party A, represented by the [Name of Party A], concludes a data access agreement with the data User’s home institution.

The researcher’s institution must agree that researchers on the project will abide by all [Name of Party A] confidentiality, disclosure analysis procedures and all relevant legal requirements.

*APPENDIX C: Available Research Data

Party A will provide factually anonymous data that can be accessed on-site via the Party B Safe Room. The factually anonymous data will be provided on a project-specific basis. The determination of whether research data are factually anonymous is at the sole discretion of Party A.

Party B and their employees refrain from any kind of interference in this matter.

*APPENDIX D: Fees

No fees are charged for Party A, Party B or the researchers accessing Party A data via the Party B Safe Room.

APPENDIX E: Relevant Legislative Texts

This Appendix contains a list of documents relevant to the legislative framework of this agreement.

[Country] and EU Legislation:
[Name of the documents and links to these documents, if available online, otherwise provide as attachments]

[Name Party A] Internal process/ procedure documents:

[Name of the documents and links to these documents, if available online, otherwise provide as attachments]

*APPENDIX F: Pledge on Data Secrecy

This Appendix provides the text that prospective Users must fulfil prior to being able to access data. The Agreement must be signed by the User and their organisation, and returned before the User can receive access credentials: username and password. The Agreement demonstrates that the prospective User and their organisation understand the seriousness of the undertaking, and that they each understand the penalties that may be imposed for non-compliances with security or confidentiality.

The Declaration is to be agreed and signed by the applicant, who will be the User requiring access to the information for his/her own research needs, and by an appropriate officer (in the Research & Contracts Office, or equivalent) from the organisation where they are based.

By signing this Declaration, I, the User, confirm that:

- I have read, understood and agreed to the [Name of Agreements signed] available at: [link to the forms]
- I have read, understood and agreed to the [Name of the Policy] available at: [link to the Policy]
- the accuracy of any information I provide to support my application
- I have read and understand the conditions specified in this Agreement
- I will abide by any other requirements communicated to me by the Party A relating to the use of potentially disclosive/Personal Information
- I will comply with all of the policies and operating procedures presented to me in the training session

I declare that the Personal Information provided to me shall be kept secure and confidential according to the terms of this Agreement.

I understand that:

- Party A may hold and process information submitted by my application for validation and statistical purposes, and for the purposes of the management of the service and may also pass such information to other parties such as data owners and data depositors.

- Party A reserves the right to scrutinise any analytical outputs, products or publications for disclosure control purposes before publication.
- I may be liable to criminal prosecution under the Statistics and Registration Service Act 2007 if I disclose Personal Information without written authority.
- I and my organisation may be liable to the Penalties outlined in [Name of the policy document] if I disclose Personal Information without the written authority of Party A.
- My lawful use of Personal Information is only for the purposes of statistical research that will serve the public good.
- Any information accessed through Safe Room will only be used for the purpose stated in the project application.
- I am required to bring directly to the attention of Party A any matters or events that may affect my obligations under this declaration.
- I am authorised to access Personal Information only when I receive from Party A a written confirmation, and only until the end date in that written confirmation.

User's signature	
User's full name and title	
Organisational address	
Date	

I, as organisational signatory, confirm that the User is attached to my organisation and understand that said organisation could be liable to the penalties outlined in the UK Data Service Licence Compliance Policy in the event of a breach of this Agreement by the User.

Organisational signature	
Name of organisational signatory	
Position of organisational signatory (must be an authorised signatory of the organisation)	
Date	

APPENDIX G: Responsibility within Party B

This Appendix specifies where responsibility lies within Party B for the tasks specified in Section 2:

Administrative and IT staff will support the following tasks of Setup/Installation and Maintenance specified in Section 2.

The operation of the Safe Room, in particular the tasks of Access control/monitoring of the Safe Room, Support and Maintenance specified in Section 2 will be carried out by staff of Party B.