

Research and Innovation Action

Social Sciences & Humanities Open Cloud

Project Number: 823782

Start Date of Project: 01/01/2019

Duration: 40 months

Deliverable 5.12 International Secure Data Facility Professionals Network (ISDFPN)

Dissemination Level	PU
Due Date of Deliverable	30/04/2022, M40
Actual Submission Date	30/04/2022, M40
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.32

Abstract:

The 'International Secure Data Facility Professionals Network' (ISDFPN) has been set up as part of the SSHOC Task 5.4 with the aim of bringing together international colleagues working in or towards Secure Data Facilities, to share expertise and experiences, discuss relevant areas of our work, and to spark collaboration as well as develop new ideas.

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. This deliverable is licensed under a Creative Commons Attribution 4.0 International License.



History

Version	Date	Reason	Revised by
0.1	24/03/2022	First draft	Beate Lichtwardt
0.2	24/03/2022	Second draft	Deborah Wiltshire, and Beate Lichtwardt
0.3	25/03/2022	Summary existing platforms	Elizabeth Lea Bishop
0.4	27/03/2022	Third draft	Deborah Wiltshire, and Beate Lichtwardt
0.5	28/03/2022	Submission	Beate Lichtwardt
0.6	29/03/2022	External peer review and comments	Neil Murray, NMurray@diw.de
0.7	29/03/2022	Implementation comments External Review Neil Murray, and further edits	Beate Lichtwardt, Deborah Wiltshire, and Elizabeth Lea Bishop
0.8	30/03/2022	Materials and comments from 1st ISDFPN online Meeting on 30th March 2022 added, further amendments	Beate Lichtwardt
0.9	04/04/2022	Edits	Elizabeth Lea Bishop, and Deborah Wiltshire
1.0	05/04/2022	Final amendments and edits	Beate Lichtwardt

Author List

Organisation	Name	Contact Information
UK Data Service/ UKDA, University of Essex	Beate Lichtwardt	blicht@essex.ac.uk
GESIS - Leibniz Institute for the Social Sciences	Deborah Wiltshire	Deborah.Wiltshire@gesis.org
GESIS - Leibniz Institute for the Social Sciences	Elizabeth Lea Bishop	ElizabethLea.Bishop@gesis.org

Executive Summary

The purpose of this report is to describe the motivation and set up of the International Secure Data Facility Professionals Network (ISDFPN), its aims, first steps, and future plans.

ISDFPN has been set up as part of the [Social Sciences and Humanities Open Cloud project \(SSHOC\)](#) Task 5.4 with the aim of bringing together international colleagues working in or towards Secure Data Facilities, to share expertise and experiences, discuss relevant areas of our work, and to spark collaboration as well as develop new ideas.

Whereas various international networks and collaborations exist, which aim to improve the international data infrastructure and landscape, and establish connections between Secure Settings, there is also a Forum needed for professional staff working in these Secure Data Facilities¹, which provides a platform for and facilitates regular knowledge exchange. ISDFPN is not a Network to establish remote connections between Secure Data Facilities but a Forum to share experience, expertise, and ideas, which is not available (yet) formally somewhere else. As the fast-changing secure data landscape evolves, this Network has been designed to be a vital resource for collaborative work towards solutions for shared as well as newly emerging problems staff faces when working in Secure Data Facilities. Nationally as well as internationally, these Secure Data Facilities are at different stages in their development, which makes such a Network a good Forum for learning from one another.

The International Secure Data Facility Network held its first online meeting on 30 March 2022, introducing the Network and its aims and objectives, discussing possible topics of interest for the Network, and establishing whether the invited parties have an interest in joining this Network. Further, a first topical session on Secure Data Facility staff skills and training needs was run, and a plan agreed for its first year 2022/2023.

Even though SSHOC finishes at the end of April 2022, this Network will be taken forward in joint collaboration between the UK Data Service and GESIS Leibniz Institute for the Social Sciences. So far, it has 22 members from 13 different institutions. The next meeting will take place on 7 September 2022.

¹ Increasingly, personal/confidential, and sensitive data are made available through Secure Data Facilities which can be also referred to as Secure Access Facilities/ Secure Research Facilities/ Safe Settings/ or Trusted Research Environments (TREs). Examples for these are a) Research Data Centres (RDCs), e.g., the IAB FDZ, RDC LiFiBi, RDC SOEP, b) Datalabs, such as the UKDS SecureLab, HMRC Datalab, ONS SRS, Justice Data Lab etc., and c) Data Safe Havens, to name just a few.

Abbreviations and Acronyms

CASD	The Secure Access Data Center
CLARIAH	Common Lab Research Infrastructure for the Arts and Humanities
EOSC	European Open Science Cloud
FORS	Swiss Centre of Expertise in the Social Sciences
GESIS	GESIS Leibniz Institute for the Social Sciences
IAB FDZ	Research Data Centre of the Federal Employment Agency at the Institute for Employment Research
LifBi	Leibniz Institute for Educational Trajectories
NSI	National Statistical Institute
ONS SRS	Office for National Statistics Secure Research Service
RDC	Research Data Centre
RDC-LifBi	Research Data Center at the Leibniz Institute for Educational Trajectories
RDC SOEP	Research Data Centre of the Socio-Economic Panel
SDC	Statistical Disclosure Control
SRT	Safe Researcher Training
TRE	Trusted Research Environment
UKDA	UK Data Archive
UKDS	UK Data Service (Service Provider in the UK - lead by UKDA)
UKDS SecureLab	UK Data Service SecureLab

Table of Contents

1. Introduction	6
2. SDAP - an example of a national network from Secure Data Professionals for Secure Data Professionals	8
2.1 History	8
2.2 Resources	8
3. The International Secure Data Facility Professionals Network (ISDFPN)	9
3.1 Terms of Reference (ToR)	10
4. ISDFPN - Meeting One	11
4.1 Agenda	12
4.2 The International Secure Data Facility Professionals Network (presentation)	12
4.3 SDAP - Competency Framework (presentation)	12
4.4 Staff skills and training needs	13
4.5 Ideas for future topics	14
4.6 Membership interest	14
5. Outlook	15
6. References	16
7. Appendix	17
Appendix 1: ISDFPN - Terms of References	17
Appendix 2: ISDFPN - Meeting One, Agenda	19
Appendix 3: ISDFPN - Meeting One, slides	20
Appendix 3.1: The International Secure Data Facility Professionals Network (ISDFPN) - slides	20
Appendix 4: ISDFPN - Meeting One, Padlets	29

1. Introduction

Enabling safe, efficient, and impactful research on societal challenges is crucial to facilitate evidence-based policy development and effecting positive change for daily lives and livelihoods within and across countries. In order to provide the foundation for such essential research, increasingly more Secure Data Facilities enable access to very detailed microdata.

It was the National Statistical Institutes (NSIs) that took the lead in the early 2000s in setting up physical Safe Rooms to make their more sensitive microdata available for research purposes on-site. Other actors followed suit in establishing Safe Rooms for accessing sensitive social science data on-site, including several national data archives (e.g., UKDA and Microdata Online Access (MONA) – Statistics Sweden), and research institutes (e.g., RDC-LifBi). In this way, Safe Rooms became more common in the Social Sciences in Europe. By 2019, numerous NSIs were offering remote access to microdata, and in 2021, the European Statistical System Committee decided to develop remote access to European secure use files, which previously could only be accessed on-site by travelling to the Eurostat Safe Center in Luxembourg.

Increasingly, Secure Data Facilities of more countries are working towards enabling remote researcher access to controlled microdata as opposed to on-site access. This can take different forms, such as remote desktop access or remote job execution.

In the UK, for the past 10 years, the UK Data Archive has successfully enabled remote access to its controlled data via the UKDS SecureLab. It plays a longstanding part in the UK data provision landscape. Initially called the Secure Data Service (SDS), this service broke new ground for data access by removing the need to travel to a fixed location for accessing detailed microdata, and 'secure remote access to data in the UK was born' (Welpton, 2021). UKDS SecureLab was the first national Secure Data Facility² providing accredited researchers with secure remote access to controlled data, including a wealth of linked longitudinal datasets. Following UKDS SecureLab provision and best practice, other TREs in the UK – for instance, the Office for National Statistics' (ONS) Secure Research Service (SRS) – now started to offer remote access for their users. UKDS SecureLab has therefore 'provided the blueprint' (Welpton, 2021) for secure remote data provision in the UK. Research productivity has increased due to ease of access, analytical outputs can be produced faster and published sooner, while research grants are no longer drained by travel expenses.

In Germany, selected Research Data Centres (RDCs) also enable remote access. For example, the Research Data Center at the Leibniz Institute for Educational Trajectories (RDC-LifBi) prepares and disseminates survey data from the German National Educational Panel Study. More sensitive versions of the data are made available via RemoteNEPS, their remote desktop system, whilst the most sensitive data remain accessible via their Onsite Data Security room in Bamberg. GESIS Leibniz Institute for the

² or Trusted Research Environment (TRE)

Social Sciences has provided access to sensitive data via its Secure Data Center Safe Room, a physical data enclave, since 2013. In 2020, a new programme of work started at the Secure Data Center to develop a new remote desktop access system. This will remove the need for researchers to travel, often some distance, to the Safe Room in order to access these data. Instead, researchers will be able to work from their own institutions, and will be able to work more flexibly, free from the constraints of having to book specific days and times to work.

Already in the 2000s there were a few small-scale initiatives to enable Safe Room Remote Desktop Access in order to reduce travel needs and facilitate access to data across borders. In this way, researchers could visit a Safe Room in one country to remotely access sensitive data from a Secure Data Facility in another country.

The Research Data Centre of the Federal Employment Agency at the Institute for Employment Research (IAB FDZ/ IAB RDC) is one example, having opened an access point at the ICPSR in 2004, and now having access points in many Safe Room locations at various Secure Data Facilities, nationally as well as internationally³.

The International Data Access Network (IDAN⁴), founded in 2018, is a collaboration between six Research Data Centres from France, Germany, the Netherlands, and the United Kingdom to facilitate research use of controlled access data via reciprocal provision of Safe Room Remote Desktop Access.

Due to limited funding, legal barriers, and other challenges, most of the infrastructure development for remote access has occurred in a bottom-up fashion, mostly on an individual institutional level or else with small-scale bilateral collaborations. Further, NSIs have little incentive to invest in infrastructure for social science researchers (this usually not being in their mandates), and national data archives generally have other priorities and limited resources to invest in remote access.

Nonetheless, the growing list of working facilities and the corresponding demand from researchers should be seen as a positive. While they do not yet meet the comprehensive list of essential requirements for SSH, they do provide proof cases that both the demand for the service is high and that the necessary technologies exist. More substantial and sustained support for a network of secure data professionals could do a great deal to advance and support these developments.

With the international data landscape fast evolving and changing, staff working in Secure Data Facilities need a means of exchanging knowledge and learning from one another. In the UK, a long-established network, the Secure Data Access Professionals (SDAP), provides such a forum for professionals working in secure data facilities across the UK. **The International Secure Data Facility Professionals Network** aims to provide such a Forum internationally.

³ [Das Forschungsdatenzentrum der BA im IAB - Locations](#) [Access 05/04/2022]

⁴ <https://idan.network> [Access 05/04/2022]

2. SDAP - an example of a national network from Secure Data Professionals for Secure Data Professionals

2.1 History

SDAP started in 2011 as a very informal gathering of data access professionals working in Secure Data Facilities across the UK. Early members came primarily from the consortium of organisations tasked with making ONS data and Longitudinal Studies data available. The group's original aims were to support professionals working within a very specialised sector. This work comes with unique tasks, and little training or support exists to help Secure Data Facility professionals develop their skills and advance their careers. All training was 'on the job' with support provided only by their fellow colleagues.

One of the primary aims of SDAP remains professionalising the work of Secure Data Facility professionals and giving them a Forum where they can exchange experiences and expertise with peers from across the sector.

This network is now well established, and currently has around 50 members from across the UK. The group meets quarterly, and all activities and future planning are overseen by a steering committee. Participation in this group has brought many benefits to its members, not least in providing a Forum where they can talk about their work and where they can bring issues to gain expert advice from others familiar with the regulatory landscape within which they work.

2.2 Resources

SDAP not only provides vital support to Secure Data Facility professionals, but through its members has produced a number of important deliverables that are widely used throughout the sector. Key deliverables are focused in three main areas: researcher training, staff skills and competencies, as well as Statistical Disclosure Control (SDC).

In the UK it is often a mandatory requirement for researchers to receive some form of training prior to gaining approval to access secure data. Even where this is not mandatory, many Secure Data Facilities are now looking at developing their own training. SDAP members from Cancer Research UK, and The Health Foundation, for example, have developed a set of canonical training materials⁵ that can be downloaded and adapted as needed.

Another important part of the work of SDAP has been to approach the area of staff skills and development. This is perceived as an important area to address as staff often come into the sector more by accident than design, and whilst they gain considerable skills through their work, the role of

⁵ <https://securdatagroup.org/training2/> [Access 05/04/2022]

the Secure Data Facility professional has not been professionalised. Opportunities for further development can be sparse. Since 2016, SDAP have been working to develop a Competency Framework⁶. The Competency Framework sets out the skills required for staff working in Secure Data Facilities and can aid staff development as a way of setting objectives, identifying strengths and areas for improvement, performance management, and preparing for future roles within the sector. It also designed to assist Secure Data Facilities with the process of recruiting new staff.

In 2017, SDAP began writing a new guide to Statistical Disclosure Control. There had been previous guides available, however these were by then some years old, and whilst the primary theoretical principles of SDC have changed little, new methodologies and data types meant that a review of SDC techniques was required. The review of this work was the publication of the SDC Handbook⁷ in 2019, followed by its translation into Spanish in 2020. The SDC Handbook was widely applauded and is considered the main 'go to' guide for Secure Data Facility professionals responsible for carrying out SDC.

Other resources available via the SDAP website include presentation slides from previous meetings and events⁸, which might be interesting and informative for Secure Data Facility professionals outside of the SDAP group.

3. The International Secure Data Facility Professionals Network (ISDFPN)

A large part of the work of SSHOC has been to expand the opening of access to secure data across international borders. This means that Secure Data Facility professionals are stepping into new, uncharted territory. As such, there is an emerging need to provide a space for Secure Data Facility professionals internationally to meet one another, to exchange knowledge, and discuss pertinent issues arising from these new connections.

There are examples of networks across Europe and beyond with the specific purpose of bringing professionals from different organisations together. A national example is RDCNet⁹ which aims to bring together participating Secure Data Facility partners from across Germany. Across countries, the International Data Access Network (IDAN)¹⁰ includes six Secure Data Facilities from the United Kingdom,

⁶ https://securedatagroup.files.wordpress.com/2018/07/sdap_competency_framework-01_00.pdf [Access 05/04/2022]

⁷ <https://securedatagroup.org/sdc-handbook/>. Some of the authors discussed the reception of the SDC Handbook in this blog published on the UKDS website (<https://blog.ukdataservice.ac.uk/statistical-disclosure-control-handbook-spanish/>) [Access 05/04/2022]

⁸ <https://securedatagroup.org/events/> [Access 05/04/2022]

⁹ <https://www.konsortswd.de/en/konsortswd/the-consortium/services/rdcnet/> [Access 05/04/2022]

¹⁰ <https://idan.network/> [Access 05/04/2022]

Germany, France, and The Netherlands. However, their primary focus lies on practical outcomes for developing infrastructure or establishing cross-organisational connections rather than on providing support and development for the practitioners. There remains no Forum for Secure Data Facility professionals internationally to share experience and expertise which is not available formally somewhere else. This is even more important as there is no definitive career path preparing staff to work in these Secure Data Facility environments. As more international bilateral connections are set up, an international Forum is needed to aid the Secure Data Facility professionals tasked with the setting up and managing of these connections.

Infrastructures must, of course, provide essential ‘plumbing’ - hardware, software, platforms, resources, and so on. However, without adequate human support (FTEs, skills, training, etc.), too often infrastructures are built but not adopted, embraced but not established, or started but not sustained. And by nature of their specialist niche, Secure Data Facility professionals tend to be widely distributed, sometimes it is only a single individual within a large institution. Therefore, improving human networks is essential. Even for well-established national Secure Data Facilities, a substantial amount of work and expertise is required to enable (Safe Room) Remote Desktop Access across borders.

Often, just a few members of staff are available to deal with all aspects of Secure Data Facilities, with no career trajectory in place to prepare for that, little organised training available to provide continuous and adequate training on the job, and too few opportunities for knowledge exchange with colleagues of other Secure Data Facilities.

In the UK, the Safe Data Access Professionals Group has worked towards filling that gap over the last 11 years, with impressive success. ISDFPN sets out to provide that much needed Forum for the international Secure Data Facility community.

3.1 Terms of Reference (ToR)

In this section the main points of the Terms of References of ISDFPN are described. Prior to the first ISDFPN Meeting, Terms of Reference (ToR)¹¹ were drafted, ready for discussion and comments during the first meeting. The timing and frequency of meetings (Steering Group Meetings, topical Member Meetings) are outlined in the ToR, and the chair and secretariat named.

The ToR contains the following objectives and deliverables.

The Objectives of ISDFPN are to:

- set strategic direction for the ISDFPN,
- oversee the achievement of deliverables,
- establish ISDFPN as an ongoing forum within an international context,

¹¹ Please see Appendix 1 for the complete ToR draft.

- run topic-based networking and knowledge exchange events for both ISDFPN members and the wider community of Trusted Research Environment (TRE) professionals,
- ensure collaboration with other professional groups where appropriate, and
- foster continued collaboration amongst ISDFPN members and the wider community of TRE professionals.

Its Deliverables are to:

- establish a Steering Group for ISDFPN,
- agree an annual calendar of meetings and events for ISDFPN members and the wider community of TRE professionals,
- identify strategic needs and set up work strands with associated projects¹²,
- agree and oversee the communications and digital strategy,
- agree a basic action plan (annual planner including all meetings, events, and work strands),
- host networking and knowledge exchange events online for ISDFPN members and the wider TRE community, informed by the work strand themes,
- develop a Community Code of Conduct for ISDFPN members and for all external public facing forums, e.g., events, social media platforms.

Further work strands will be established over time, and the members involved recorded. These may change from year to year, in response to changes in the international secure data access landscape.

4. ISDFPN - Meeting One

The International Secure Data Facility Professionals Network held its first meeting on 30 March 2022. Twenty-two people from 13 different institutions, and 5 countries registered to attend this meeting. In addition, further parties have expressed interest, even though they were not able to attend the initial meeting.

This section will briefly comment on the meeting, including its agenda, presentations, two Padlet¹³ tasks, and its outcomes.

4.1 Agenda

The agenda of the first meeting included the following items (Please see Appendix 2 for the complete Agenda):

¹² Projects within these work strands may be led by a Steering Group member, or by an ISDFPN Group member, with involvement from a Steering Group member.

¹³ This is a cloud-based software-as-a-service, hosting a real-time collaborative web platform in which users can upload, organise, and share content to virtual bulletin boards called 'padlets'.

- Welcome and introductions
- International Secure Data Facility Professionals Network (ISDFPN) – presentation
- SDAP Competency Framework - presentation
- Discussion: Training needs of Secure Data Facility staff (Padlet)
- Expression of interest for ISDFPN membership, and Identifying topics for future meetings (Padlet)
- Any Other Business.

4.2 The International Secure Data Facility Professionals Network (presentation)

The presentation opened with an overview of the SSHOC project. The Work Package was also presented, with emphasis on the diversity of disciplines involved, from biomedical data to heritage resources. The subtask 5.4 on Remote Access was explained, including some of the deliverables likely to be of interest to participants, such as a practical legal template. The first part concluded by noting that strengthening human networks of secure data professionals is essential for this work and will be a key recommendation from the subtask. Having made the case for the need for an International Secure Data Professionals Network, its objectives and deliverables were discussed next, followed by an outlook.

4.3 SDAP - Competency Framework (presentation)

One of the resources the UK Working Group for Secure Data Access Professionals (SDAP) created, is the Competency Framework. Its intended use was for staff development and recruitment purposes by setting objectives, identifying skills, and planning career progression. The presentation addressed the issues data professionals in Secure Data Facilities face, whether the Competency Framework is still relevant or whether there are skills not mentioned back then which would be mentioned now, what training would be needed to enable career progression, and how such a career progression could look like.

4.4 Staff skills and training needs

Two Padlet exercises formed part of the agenda for the first meeting of the International Secure Data Facility Professionals Network, the first focusing on 'Staff skills and training needs'.

This exercise followed the presentation on the Competency Framework developed by the UK SDAP Group, setting the scene for the discussion on staff skills and training needs in Secure Data Facilities.

The following four questions had been placed in the Padlet.

- Are there skills missing at this point in time?
- What training is needed? Does this exist, and, if so, where?
- What skills might the Secure Data Facility professional of 2032 need?
- Other thoughts/ comments?

The current missing skills listed by attendees included machine learning and AI; programming of statistics software; anonymisation and pseudonymisation tools; awareness of synthetic data techniques; talking to data holders; workflows for ingesting data; research reproducibility; and knowledge regarding non-tabular data.

The training needs identified included an overview of Secure Data Facilities offering remote access and to which data sources, and training on IT requirements for a non-technical audience. Existing resources highlighted included the Output Checker Course (DRAGon), the Safe Researcher Training (SRT), FAIR data stewardship, SDAP's Statistical Disclosure Control Handbook, Summer School courses on data management, and certificates for training participation.

Asking participants what skills a Secure Data Facility Professional of 2032 might need resulted in the following answers: confidence, awareness of ethical complexities in outputs, and automation of low-level outputs. It was great to see that participants anticipate that international data sharing will have become increasingly common in 10 years' time.

Other thoughts turned to the need to increase the recognition and pay of staff involved in Secure Data Facility tasks such as Statistical Disclosure Control (SDC), and the lack of a professionalisation of their roles. That was supported by the fact that SDC decisions can have major legal implications and thus warrant these calls for recognition and professionalisation. Further comments suggested a diversification of roles might be required within Secure Data Facilities to reflect the increasing complexity of services involved.

4.5 Ideas for future topics

A second Padlet exercise focused on establishing 'Ideas for future topics'. This was an important first step towards identifying possible work strands for the first year of the Network. Going forward, each meeting will be designed to discuss current issues as well as having a presentation on a topic of interest to the group. Mentioned in the Padlet, amongst others, were the following suggestions:

- Overview of existing Secure Data Facilities/ Secure Data Facility Infrastructure
- Overview services involved in ISDFPN
- Future direction ISDFPN
- Overview available remote access to (which?) data (at present)
- Access systems for secure data (IT solutions)
- Automatization of Secure Data Facility tasks (e.g., output checking; self-administration platforms for users)

- Public Engagement and involvement
- Legal questions (GDPR supporting remote secure data access)
- Authorisation procedures
- Qualitative data in Secure Data Facilities
- Resources/ Knowledge bank.

This list gives the Network plenty to work with. It becomes quite clear that members wish to start with an inventory of what is available at present, and in what direction the group should be heading. This is closely followed by the need for advice on best practice regarding IT solutions; legal questions; and solutions to manage the workload (for example in terms of administration and output checking). Comparatively new areas, such as qualitative data in Secure Data Facilities, are another point of interest for the group. Finally, it was suggested that a practical starting point for this international Network would be the collection of existing resources, either provided by members of the group or known to members of the Network. The suggestion mentioned in the Padlet summarises that as a Resources/ Knowledge bank.

4.6 Membership interest

22 people from 13 different institutions, and 5 countries had registered for the first meeting of the International Secure Data Facility Professionals Network on 30 March 2022. Those who had been unable to attend the meeting, but who had expressed interest, will be invited for the second meeting, and will have the option of joining the Network then.

During its first meeting, representatives of the following institutions joined ISDFPN:

- UKDS/ UKDA (UK)
- GESIS (Germany)
- IAB FDZ (Germany)
- CASD (France)
- UWE (UK)
- The Health Foundation (UK)
- FORS (Switzerland)
- LfBi (Germany)
- RDCnet/ DIW (Germany)
- Radboud University (The Netherlands)
- German Cancer Research Centre (Germany)
- Dutch National Institute for Public Health and Environment (The Netherlands)
- Clariah (The Netherlands)

5. Outlook

The international Secure Data Facility community's response to the first ISDFPN meeting clearly demonstrates the need and desire for such a Network. Whilst SSHOC officially comes to an end at the End of April 2022, the Network will continue. A Steering Group has been appointed to take the Network forward and begin the work towards the deliverables. An analysis of the Padlet exercises from the first meeting will inform future work strands and meeting agendas as well as helping to identify relevant speakers for future events.

The International Secure Data Facility Professionals Network will be carried forward in joint collaboration of the UK Data Service and GESIS, under the leadership of co-chairs Beate Lichtwardt (UKDS) and Deborah Wiltshire (GESIS). The Network can be contacted at isdfpn@ukdataservice.ac.uk.

The next meeting is scheduled for 7th September 2022.

6. References

Elizabeth Bishop. (2021). MS28 Assessment of Existing Platforms (1.0). Zenodo. <https://doi.org/10.5281/zenodo.5914390>

Bishop, L., Broeder, D., van den Heuvel, H., Kleiner, B., Lichtwardt, B., Wiltshire, D., Voronin, Y., Deliverable 5.10 White Paper on Remote Access to Sensitive Data in the Social Sciences and Humanities: 2021 and beyond. (forthcoming)

International Data Access Network <https://idan.network/>

Beate Lichtwardt, Matthew Woollard, Deborah Wiltshire, & Elizabeth Lea Bishop. (2022). D5.11 ERAN Pilot: Setting up a Secure Remote Connection between two Trusted Research Environments (v1.0) (forthcoming)

RDCNet <https://www.konsortswd.de/en/konsortswd/the-consortium/services/rdcnet/>

James Scott, Beate Lichtwardt, and Christine Woods. (2022). UK Data Service SecureLab: pioneers in enabling safe data-driven research for over a decade. UKDS Data Impact blog. 12 January 2022. <https://blog.ukdataservice.ac.uk/securelab-ten-year-anniversary/>

James Scott, and Christine Woods. (2020). Statistical Disclosure Control Handbook now available in Spanish. UKDS Data Impact blog. 23 July 2020. <https://blog.ukdataservice.ac.uk/statistical-disclosure-control-handbook-spanish/>

Secure Data Access Professionals <https://securedatagroup.org/>

Richard Welpton. (2021). Celebrating 10 years of secure remote access in the UK. UKDS Data Impact blog. 12 October 2021. <https://blog.ukdataservice.ac.uk/ten-years-secure-remote-access/>

Deborah Wiltshire. (2021). D5.20 Training materials of workshop for secure data facility professionals (v1.0). Zenodo. <https://doi.org/10.5281/zenodo.5638596>

Matthew Woollard, Beate Lichtwardt, Elizabeth Lea Bishop, & Dana Müller. (2021). D5.9 Framework and contract for international data use agreements on remote access to confidential data (v1.0). Zenodo. <https://doi.org/10.5281/zenodo.4534286>

7. Appendix

Appendix 1: ISDFPN - Terms of References

International Secure Data Facility Professionals Network (ISDFPN) - Terms of Reference

Objectives - to:

1. set strategic direction for ISDFPN,
2. oversee the achievement of deliverables,
3. establish ISDFPN as an ongoing forum within an international context,
4. run topic-based networking and knowledge exchange events for both ISDFPN members and the wider community of Trusted Research Environment (TRE) professionals,
5. ensure collaboration with other professional groups, where appropriate, and
6. foster continued collaboration amongst ISDFPN members and the wider community of TRE professionals.

Deliverables - to:

1. establish a Steering Group for ISDFPN,
2. agree an annual calendar of meetings and events for ISDFPN members and the wider community of TRE professionals,
3. identify strategic needs and set up work strands with associated projects. Projects within these work strands may be led by a Steering Group member, or by an ISDFPN Group member, with involvement from a Steering Group member,
4. agree and oversee the communications and digital strategy,
5. agree a basic action plan (annual planner including all meetings, events and work strands)
6. host networking and knowledge exchange events online for ISDFPN members and the wider TRE community, informed by the work strand themes,
7. develop a Community Code of Conduct for ISDFPN members and for all external public facing forums, e.g. events, social media platforms etc..

Work strands

The work strands are set out below. These may change from year to year, in response to changes in the international secure data access landscape.

Work Strands	Steering Group members to be involved

Chair and secretariat

Co-Chairs – Beate Lichtwardt (UKDS), Deborah Wiltshire (GESIS)

Deputy Chair - Libby Bishop (GESIS)

Executive Officer - Helen Cadwallader, Membership and European Projects Officer, UK Data Service, University of Essex, will provide secretariat for the group. Papers will be distributed 5 working days before meetings by email.

Timing/frequency of meetings

The group will meet biannually. All meetings will be held online.

Work strand sub groups may need to meet when completing specific work.

Steering Group Members

Name	Organisation

Appendix 2: ISDFPN - Meeting One, Agenda

International Secure Data Facility Professionals Network (ISDFPN)

Meeting 1

Wednesday 30th March 2022, 14.30hrs to 16.00hrs (GMT)

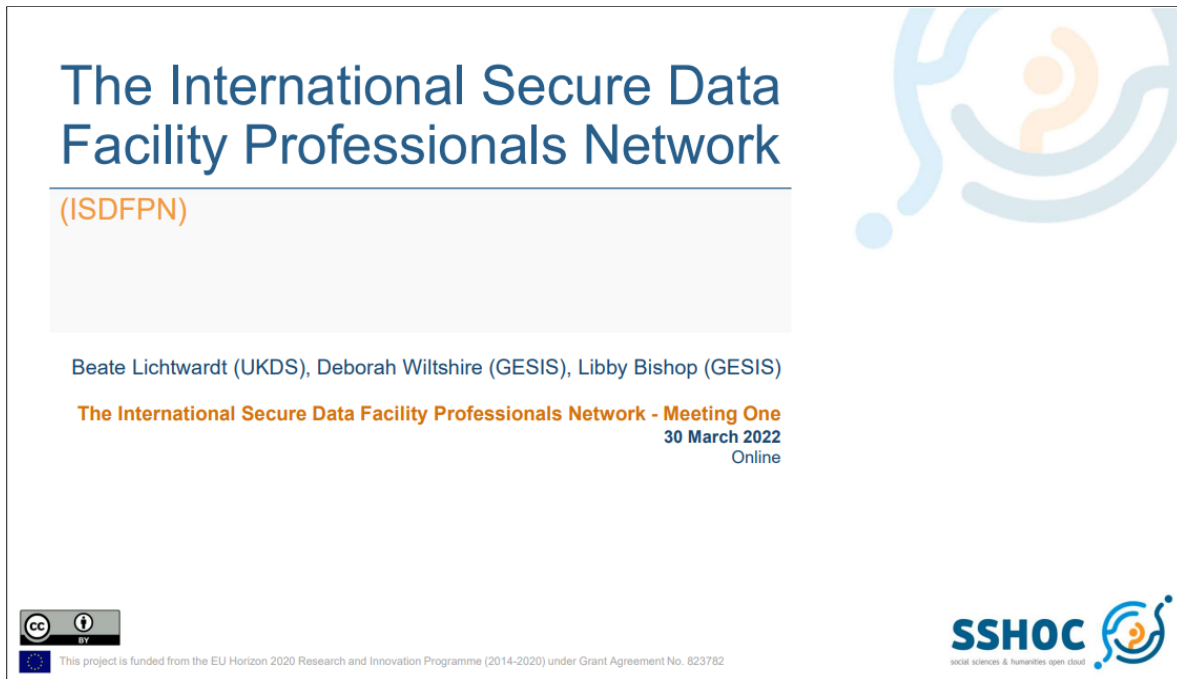
Virtual meeting by Microsoft Teams

Agenda

1.	Welcome and introductions Beate Lichtwardt (UK Data Service) - Chair	14.30hrs – 14.45hrs	BL, All (15mins)
2.	International Secure Data Facility Professionals Network (ISDFPN) – presentation Beate Lichtwardt (UK Data Service), Libby Bishop (GESIS) and Deborah Wiltshire (GESIS)	14.45hrs – 15.05hrs	BL and LB (20mins)
3.	SDAP Competency Framework - presentation Yannis Kotrotsios (The Health Foundation) Please see attached file: 'SDAP_Compentency_Framework_1.0.pdf'	15.05hrs – 15.25hrs	YK (20mins)
4.	Discussion: Training needs of Secure Data Facility Staff Reflections on: <ul style="list-style-type: none"> - Any missing skills at this point in time? - What training is needed? Does this exist, and if so, where? - What skills might the Secure Data Facility professional of 2032 need? - Other thoughts / comments? 	15.25hrs – 15.40hrs	All (15mins)
5.	Expression of interest for ISDFPN membership Identifying topics for future meetings	15.40hrs – 15.55hrs	All (15mins)
6.	Any Other Business	15.50hrs – 16.00hrs	All (5mins)

Appendix 3: ISDFPN - Meeting One, slides

Appendix 3.1: The International Secure Data Facility Professionals Network (ISDFPN) - slides




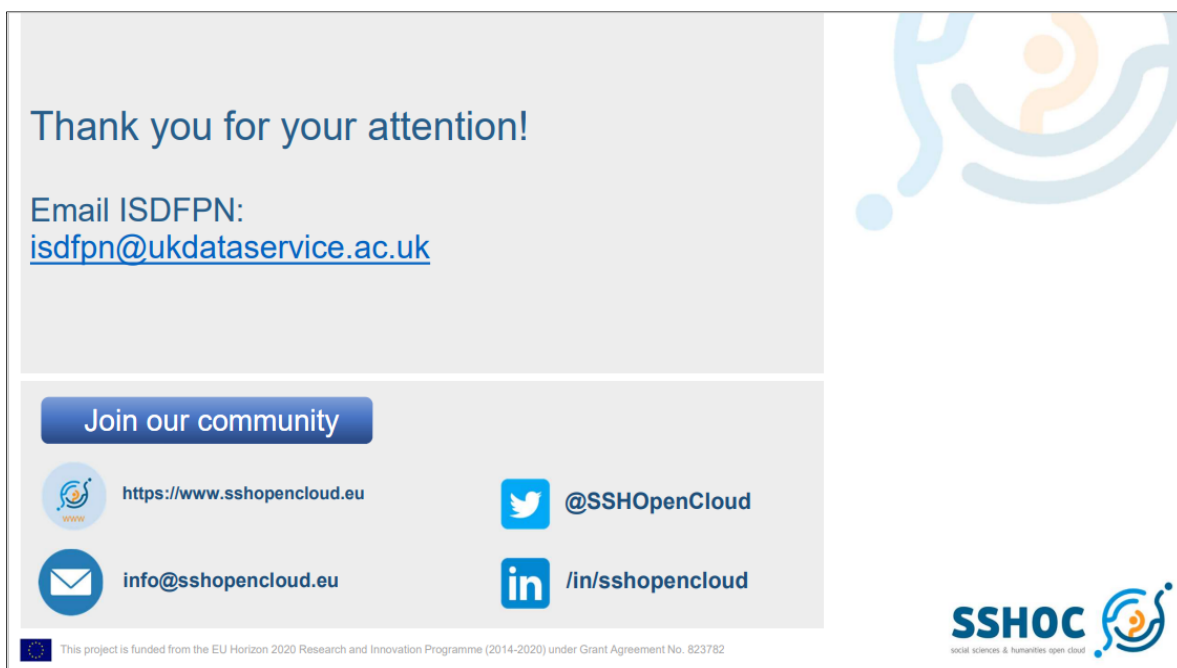

The International Secure Data Facility Professionals Network

(ISDFPN)

Beate Lichtwardt (UKDS), Deborah Wiltshire (GESIS), Libby Bishop (GESIS)

The International Secure Data Facility Professionals Network - Meeting One
30 March 2022
Online



 This project is funded from the EU Horizon 2020 Research and Innovation Programme (2014-2020) under Grant Agreement No. 823782






Thank you for your attention!


Email ISDFPN:
isdfpn@ukdataservice.ac.uk

Join our community

 <https://www.sshopencloud.eu>  @SSHOpenCloud


 info@sshopencloud.eu  /in/sshopencloud

 This project is funded from the EU Horizon 2020 Research and Innovation Programme (2014-2020) under Grant Agreement No. 823782



Roadmap

- Social Sciences & Humanities Open Cloud (SSHOC) Project - Overview
- WP5: Innovations in Data Access
- Task 5.4 Remote Access to Sensitive Data
- D5.12 International Secure Data Facility Professionals Network (ISDFPN)
- ISDFPN - Objectives and deliverables
- Outlook

 This project is funded from the EU Horizon 2020 Research and Innovation Programme (2014-2020) under Grant Agreement No. 823782

Project:



Type of action & funding:
Research and Innovation action
(INFRAEOSC-04-2018)

Partners: 47
(20 beneficiaries + 27 LTPs)
SSH ESFRI Landmarks and Projects
& international SSH data infrastructures

Project budget:
€ 14,455,594.08

Duration: 40 months
(January 2019 – 30 April 2022)

Project website:
www.SSHOpenCloud.eu



Objectives:

- creating the social sciences and humanities (SSH) part of European Open Science Cloud (EOSC)
- maximising **re-use** through **Open Science** and **FAIR** principles (standards, common catalogue, access control, semantic techniques, training)
- interconnecting existing and new infrastructures (clustered cloud infrastructure)
- establishing appropriate **governance model** for SSH-EOSC

WP5: Innovations in Data Access

Work Package 5 facilitates innovations in data access and provides tools and services for intelligently open data for the SSH domain to be incorporated into the EOSC cloud.

WP5 objectives:

- Help users to make the actual transition from their current practices to having their data openly accessible, by providing appropriate tools and representative examples;
- Develop and test protocols for data access to biomedical data linked to survey data;
- Provide data repository services for SSH institutions having limited technical resources; Develop a GDPR Code of Conduct for SSH;
- Enhance and extend the infrastructure for secure remote access to research data;
- Use the ESS to pilot how cross-national survey data and metadata can be prepared and provide services for the EOSC;
- Develop examples of making Heritage Science and archaeological data more interoperable and accessible in the SSH.

<https://sshopencloud.eu/project>



This project is funded from the EU Horizon 2020 Research and Innovation Programme (2014-2020) under Grant Agreement No. 823782

Task 5.4 Remote Access to Sensitive Data: Key Deliverables and Milestones

- M28 Assessment of existing (Remote Desktop) platforms
- D5.9 Framework and contract for international data use agreements on remote access to confidential data
- D5.20 Training materials of workshop for secure data facility professionals
- D5.11 European Remote Access Pilot (one secure remote connection)
- M29 Tested connections between partners with live data and researcher projects
- D5.10 White Paper “Remote Access to Sensitive Data in the Social Sciences and Humanities: 2021 and Beyond”- Key point from the Recommendations
- D5.12 International Secure Data Facility Professionals Network



This project is funded from the EU Horizon 2020 Research and Innovation Programme (2014-2020) under Grant Agreement No. 823782

Identifying the need for an international network of support for professionals

*Infrastructures must, of course, provide essential “plumbing” - hardware, software, platforms, resources, and so on. However, without adequate human support (FTEs, skills, training, etc.), too often infrastructures are built but not adopted, embraced but not established, or started but not sustained. And by nature of their specialist niche, secure data professionals tend to be widely distributed, sometimes only a single individual within a large institution. **Improving human networks is essential.***



This project is funded from the EU Horizon 2020 Research and Innovation Programme (2014-2020) under Grant Agreement No. 823782

5.12 International Secure Data Facility Professionals Network (ISDFPN) - Objectives

- Set strategic direction for ISDFPN
- Oversee the achievement of the deliverables
- Establish ISDFPN as an ongoing forum within an international context
- Run topic based networking and knowledge exchange events for both, ISDFPN members and the wider community of Secure Data Access or Trusted Research Environment (TRE) professionals
- Ensure collaboration with other professional groups, where appropriate
- Foster continued collaboration amongst ISDFPN members and the wider community of TRE professionals



This project is funded from the EU Horizon 2020 Research and Innovation Programme (2014-2020) under Grant Agreement No. 823782

ISDFPN - Deliverables

- Establish a Steering Group for ISDFPN
- Agree an annual calendar of meetings and events for ISDFPN members and the wider community of TRE professionals
- Identify strategic needs and set up work strands with associated projects
- Agree and oversee the communications and digital strategy
- Agree a basic action plan (annual planner including all meetings, events, and work strands)
- Host networking and knowledge exchange events online for ISDFPN members and the wider TRE community, informed by the work strand themes
- Develop a Community Code of Conduct for ISDFPN members and for all external public facing forums, e.g. events, social media platforms etc.



This project is funded from the EU Horizon 2020 Research and Innovation Programme (2014-2020) under Grant Agreement No. 823782

Outlook

- Following first meeting today, work on deliverables will start:
 - **Steering Group**
 - **Work strands 1st year**
 - **Analysis of staff training needs from today's discussion, establishing future topics of interest**
- Although SSHOC ends at the End of April 2022, ISDFPN will be carried forward in joint collaboration of UKDS and GESIS
- Next meeting: 7th September 2022



This project is funded from the EU Horizon 2020 Research and Innovation Programme (2014-2020) under Grant Agreement No. 823782

Mind the Skills Gap: Creating Capacity for Data Access

SDAP: Competency Framework - International Secure Data Facility
Professionals Network (ISDFPN)

March 2022



Yannis Kotrotsios
Senior Data Manager
Data Analytics

30 March 2022

SDAP: Competency Framework

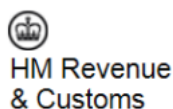


Working Group for Secure Data Access Professionals (SDAP)

- Established 2011
- Working together to improve delivery of secure access to data



UK Data Service



30 March 2022

SDAP: Competency Framework



Agreeing to make data available

- In principle:
 - ✓ Data access is possible
 - ✓ The willingness exists
- What are the practicalities for making data available?
 - ✓ Data Application
 - ✓ Legal getaways
 - ✓ Security (ISMS)
 - ✓ Technical Solution
- Who will make this happen?



30 March 2022

SDAP: Competency Framework



What's the problem?

<p>Staff take on much risk, receive little reward <i>Professional Career</i></p>	<p>Not Confident to make decisions - Staff tend to '<i>fall into roles by accident</i>'</p>	<p>Lack of investment in staff <i>No professional Development</i></p>

30 March 2022

SDAP: Competency Framework



SDAP Competency Framework

- Created back in 2018 by Carlotta Greci, Richard Welpton and Christine Woods to set out the competences for staff working in Safe Settings

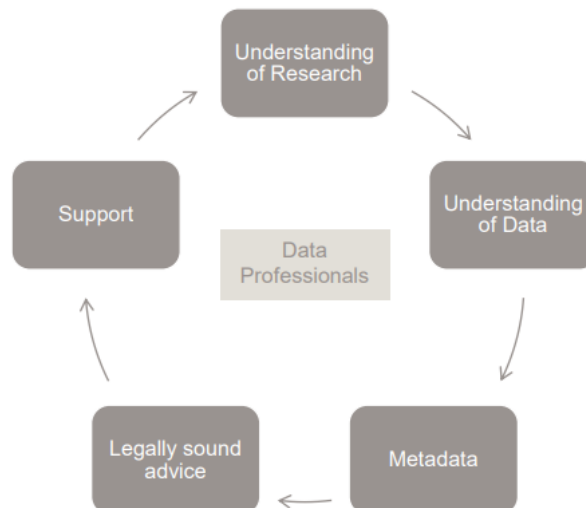
- The intention was to be used for Staff development & Recruitment
 - Setting objectives
 - Identify skills and weaknesses
 - Plan career progression
 - CRUK used the framework to create the Data Access Officer role profile back in 2018

30 March 2022

SDAP: Competency Framework



Data support for research: a profession?



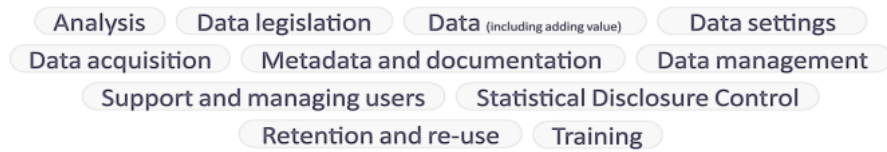
30 March 2022

SDAP: Competency Framework



Data support for research: Skills

Areas of understanding

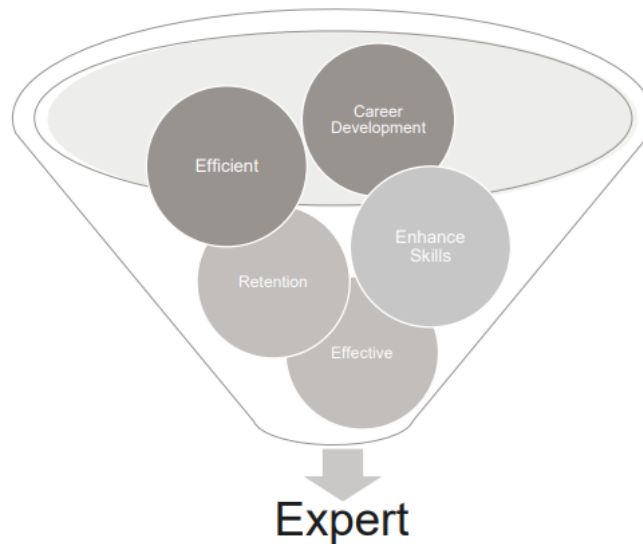


30 March 2022

SDAP: Competency Framework



Data support for research: Professional career



30 March 2022

SDAP: Competency Framework



SDAP Competency Framework - Plans

- Is the framework still relevant in 2022?
- What skills should the framework cover / are any missing?
- What training might be relevant to signpost to in the framework?
(think about training you've already benefited from / received when you started working with secure data)
- How to showcase career development?
- What might the SDAP professional of 2032 need?

30 March 2022

SDAP: Competency Framework

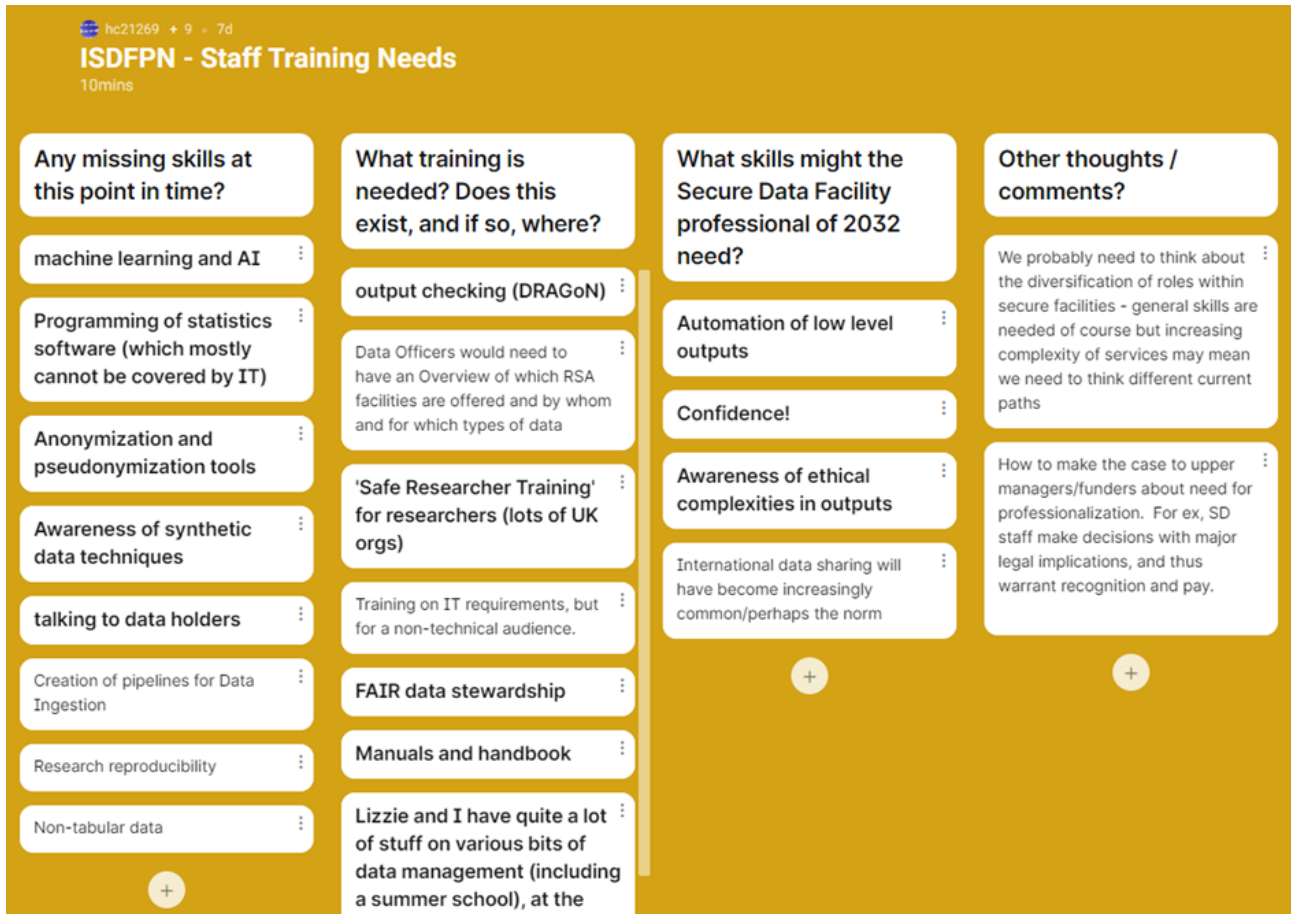


Thanks for listening



Yannis.Kotrotsios@health.org.uk

Appendix 4.1: Staff skills and training needs - Padlet



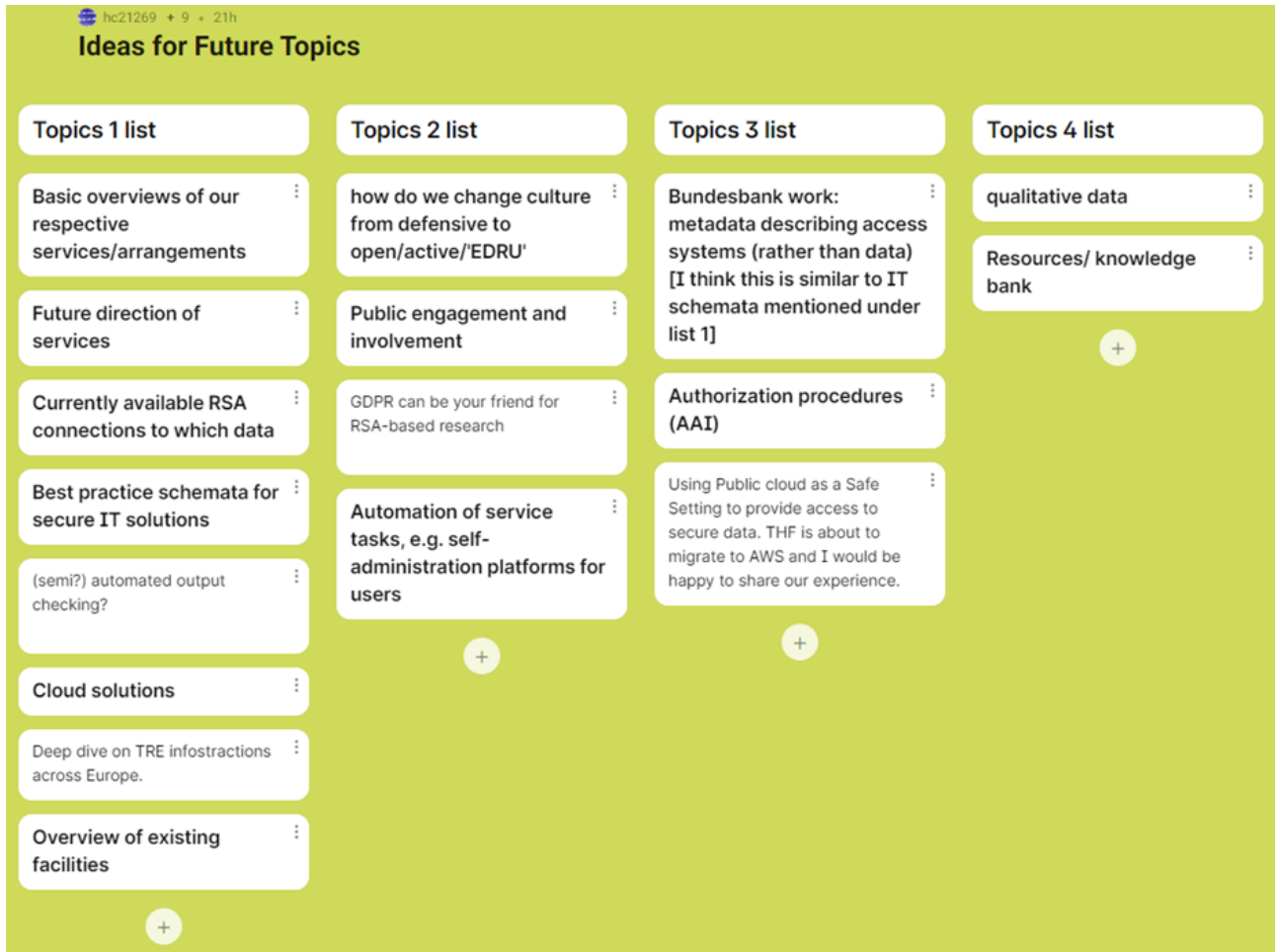
hc21269 + 9 - 7d
ISDFPN - Staff Training Needs
10mins

Any missing skills at this point in time?	What training is needed? Does this exist, and if so, where?	What skills might the Secure Data Facility professional of 2032 need?	Other thoughts / comments?
<ul style="list-style-type: none"> machine learning and AI Programming of statistics software (which mostly cannot be covered by IT) Anonymization and pseudonymization tools Awareness of synthetic data techniques talking to data holders Creation of pipelines for Data Ingestion Research reproducibility Non-tabular data 	<ul style="list-style-type: none"> output checking (DRAGoN) Data Officers would need to have an Overview of which RSA facilities are offered and by whom and for which types of data 'Safe Researcher Training' for researchers (lots of UK orgs) Training on IT requirements, but for a non-technical audience. FAIR data stewardship Manuals and handbook Lizzie and I have quite a lot of stuff on various bits of data management (including a summer school), at the 	<ul style="list-style-type: none"> Automation of low level outputs Confidence! Awareness of ethical complexities in outputs International data sharing will have become increasingly common/perhaps the norm 	<ul style="list-style-type: none"> We probably need to think about the diversification of roles within secure facilities - general skills are needed of course but increasing complexity of services may mean we need to think different current paths How to make the case to upper managers/funders about need for professionalization. For ex, SD staff make decisions with major legal implications, and thus warrant recognition and pay.

(Padlet - Staff skills and training needs, continued)

Any missing skills at this point in time?	What training is needed? Does this exist, and if so, where?	What skills might the Secure Data Facility professional of 2032 need?	Other thoughts / comments?
machine learning and AI			
Programming of statistics software (which mostly cannot be covered by IT)	'Safe Researcher Training' for researchers (lots of UK orgs)	Automation of low level outputs	We probably need to think about the diversification of roles within secure facilities - general skills are needed of course but increasing complexity of services may mean we need to think different current paths
Anonymization and pseudonymization tools	Training on IT requirements, but for a non-technical audience.	Confidence!	
Awareness of synthetic data techniques	FAIR data stewardship	Awareness of ethical complexities in outputs	How to make the case to upper managers/funders about need for professionalization. For ex, SD staff make decisions with major legal implications, and thus warrant recognition and pay.
talking to data holders	Manuals and handbook	International data sharing will have become increasingly common/perhaps the norm	
Creation of pipelines for Data Ingestion	Lizzie and I have quite a lot of stuff on various bits of data management (including a summer school), at the moment tailored to clietns but we're getting closer to generic stuff. Aiming to have generic SDC materials available on a public website and of the year		
Research reproducibility		Certificates for Training Participation	
Non-tabular data			

Appendix 4.2: Ideas for future topics - Padlet



hc21269 + 9 + 21h

Ideas for Future Topics

Topics 1 list	Topics 2 list	Topics 3 list	Topics 4 list
Basic overviews of our respective services/arrangements	how do we change culture from defensive to open/active/'EDRU'	Bundesbank work: metadata describing access systems (rather than data) [I think this is similar to IT schemata mentioned under list 1]	qualitative data
Future direction of services	Public engagement and involvement	Authorization procedures (AAI)	Resources/ knowledge bank
Currently available RSA connections to which data	GDPR can be your friend for RSA-based research	Using Public cloud as a Safe Setting to provide access to secure data. THF is about to migrate to AWS and I would be happy to share our experience.	
Best practice schemata for secure IT solutions	Automation of service tasks, e.g. self-administration platforms for users		
(semi?) automated output checking?			
Cloud solutions			
Deep dive on TRE infostractions across Europe.			
Overview of existing facilities			