Convergence Initiative

Anita Mittal , GIZ

Digital Social Protection

Information systems are indispensable for delivery of Social Protection

Social protection information systems are complex involving integration and interaction between multiple components

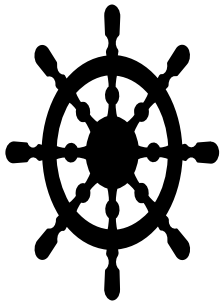
Integrated and interoperable social protection systems enable efficient, responsive service delivery

USP 2030 Vision : A world where anyone who needs social protection can

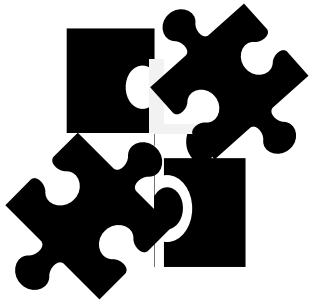
Social Registry, ID system, G2P system, integrated beneficiary registry, CRVS, Tax, Pension, Individual program information system

Targeting, eligibility, leakages, duplication, administration, user experience, adaptive social protection

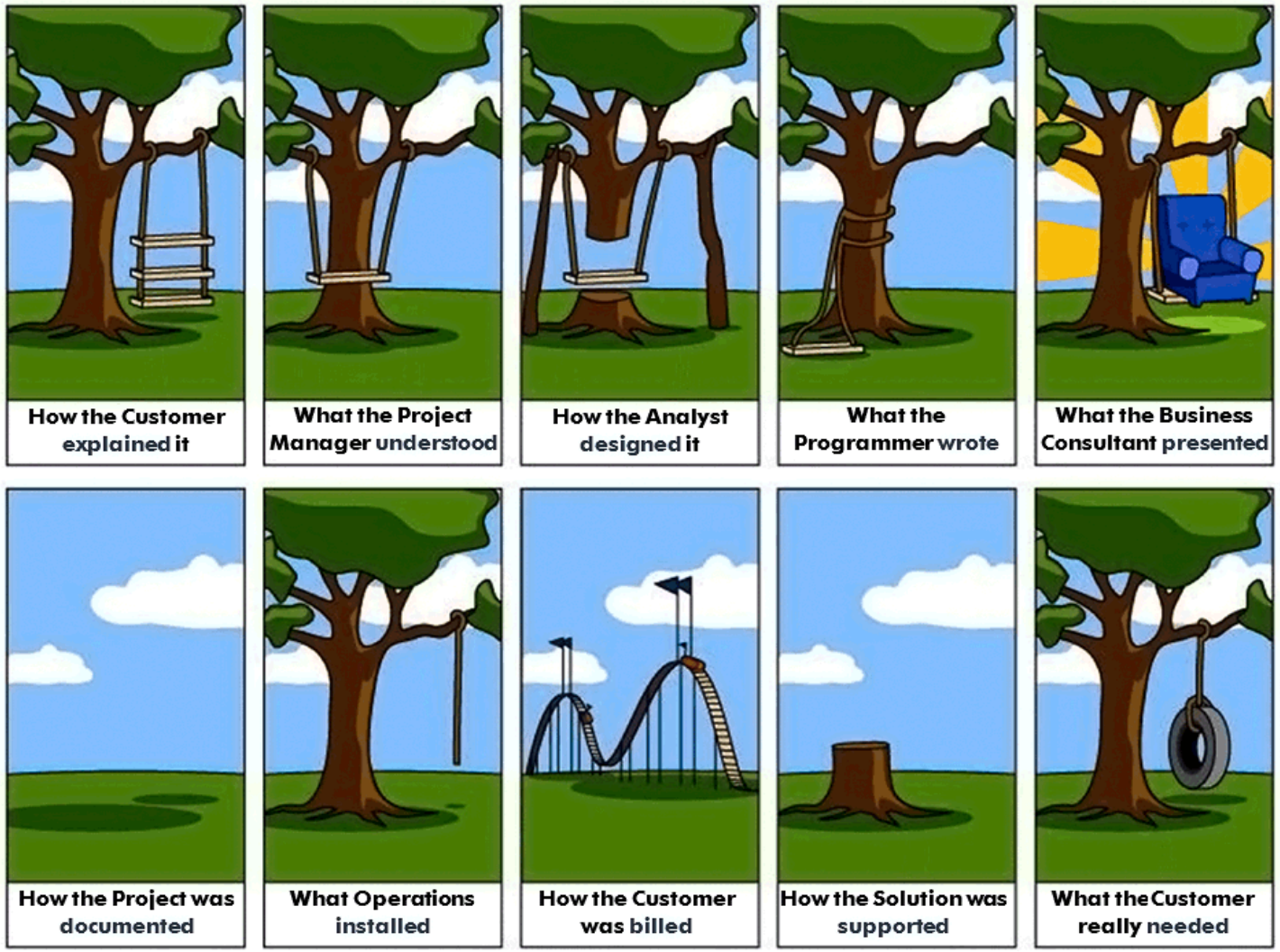
Yet the potential of information systems remains unrealized



REINVENTING THE WHEEL



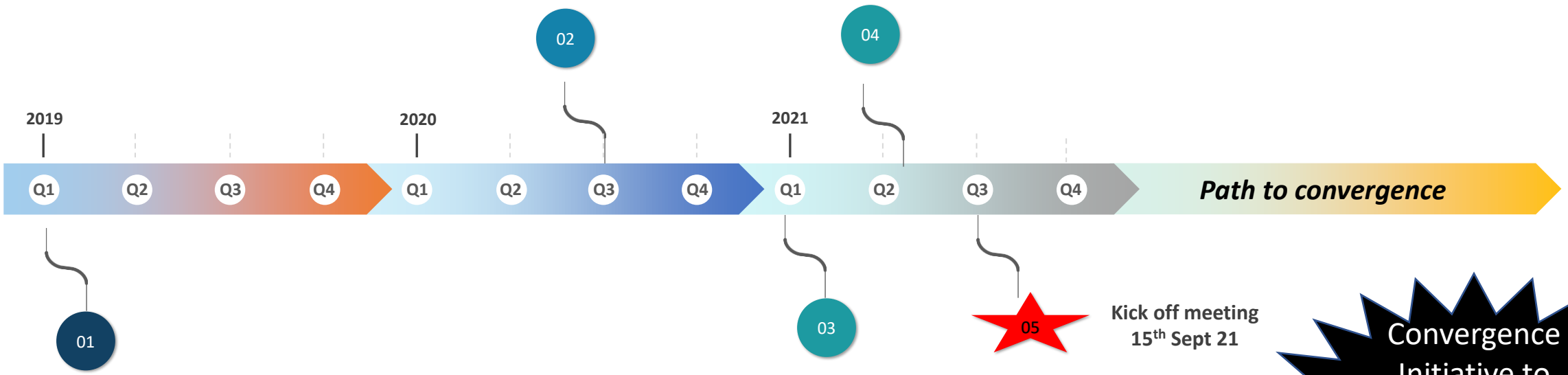
LACK OF INTEROPERABILITY



USP2030 UNIVERSAL SOCIAL PROTECTION SPIAC - B ADB ASIAN DEVELOPMENT BANK german cooperation DEUTSCHE ZUSAMMENARBEIT giz THE WORLD BANK IBRD • IDA International Labour Organization ISSA Information Systems Security Association International

Governments

Convergence of stakeholders to address the felt needs



Digital Social Protection Working Group established under the Social Protection Inter Agency Cooperation-Board (SPIAC-B)

Study commissioned to understand how the social protection sector can achieve convergence of digital systems

USP2030 membership assembly approves the pitch made by SPIAC-B on the creation of the **Convergence Initiative**

Prepare for the launch of the initiative

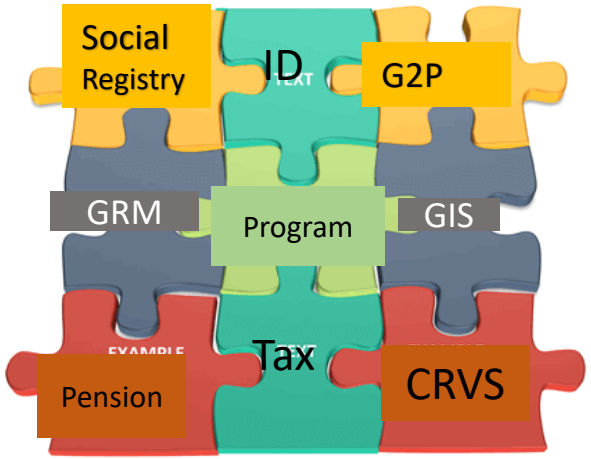
Kick off meeting 15th Sept 21

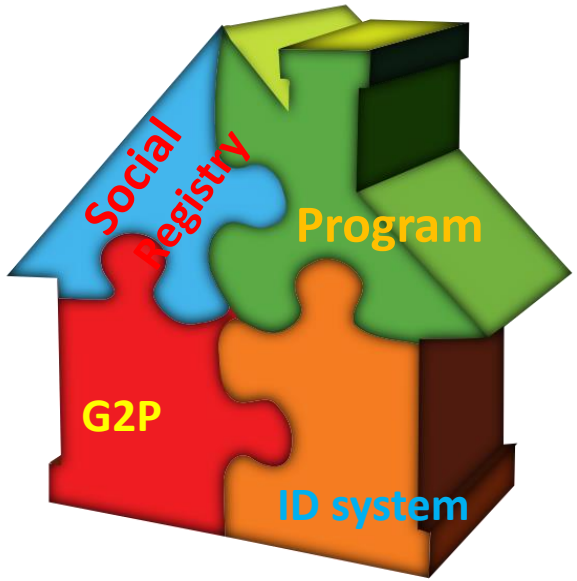
Convergence Initiative to converge on global standards for SP

Convergence Initiative Vision - Goals

- Foster an **ecosystem for innovation** by ICT solution providers to build **products that are interoperable**, based on globally agreed standards and guidelines
- **Reduce time and costs** of developing solutions at the country/program level
- Ensure that systems are **future-proof by design**, regardless of current levels of policy and information systems maturity
- Enable programs and countries to **mix and match interoperable components** from various vendors

Interactions amongst different systems for SP program delivery





MANY SECTORS HAVE PURSUED STANDARDIZATION AT VARIOUS LEVELS and REALIZED BENEFITS

Data standards for ex-post data sharing by humanitarian organizations

Common business and system requirements for civil registration and vital statistics systems

OpenHIE

Common reusable architectural framework for health information exchange. Impact stories - https://ohie.org/impact-stories/

HL7 International

FHIR

International standards for transfer of clinical and administrative data between software applications used by various healthcare providers

Successes

Common Backend for Global Goods

OPENSRP

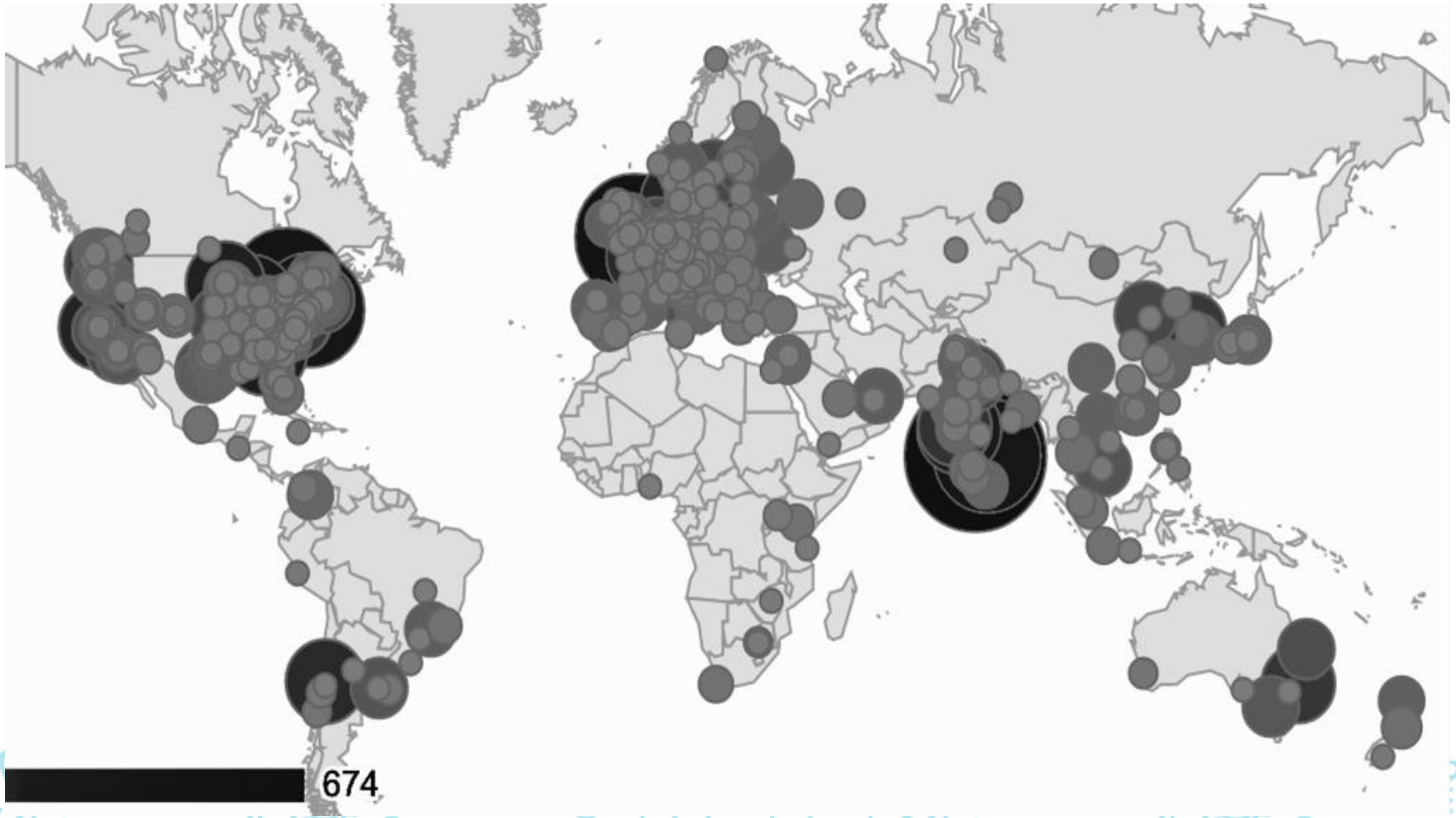
Successes: Technology For Cost Effective Care

Successes: HAPI FHIR

- HAPI FHIR is an open source implementation of the FHIR standard for:
  - National EHR Programs
  - mHealth Startups
  - Academic research programs
  - EMRs of all sizes
  - ...etc.

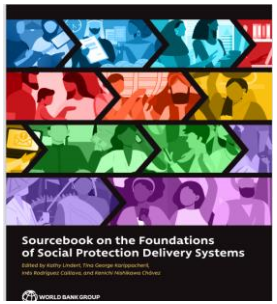
HAPI FHIR

Successes: Nearly Global Adoption



Efforts by various organizations to address interoperability and convergence on standards in Social Protection

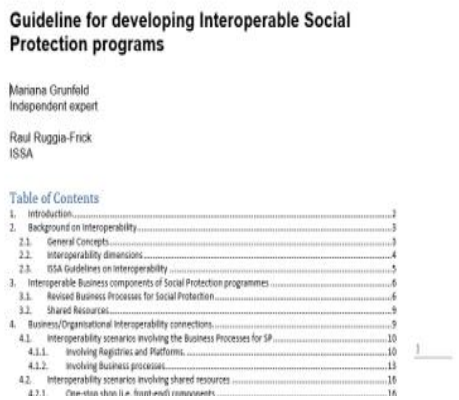
THE WORLD BANK
IBRD • IDA



Australian Government
Department of Foreign Affairs and Trade

ISSA
Information Systems Security Association International

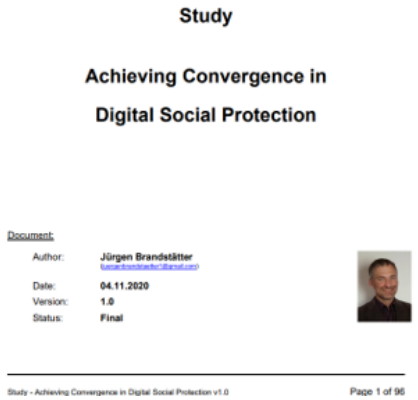
International Labour Organization


Guideline for developing Interoperable Social Protection programs

Mariana Grunfeld
Independent expert

Raul Ruggia-Frick
ISSA

Table of Contents


Study

Achieving Convergence in

Digital Social Protection

Document:

Author: Jürgen Brandstätter

Date: 04.11.2020

Version: 1.0

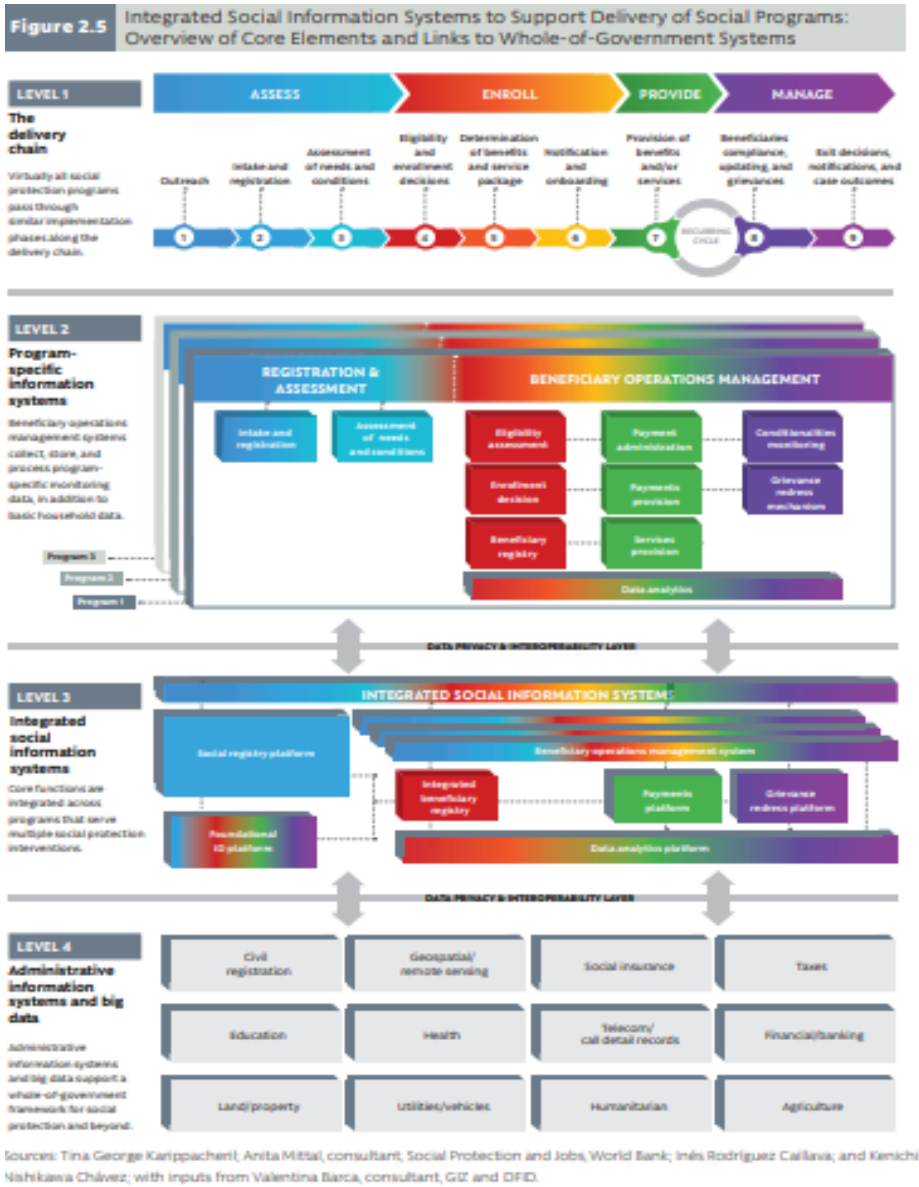
Status: Final

Study - Achieving Convergence in Digital Social Protection v1.0 Page 1 of 96

USP2030
UNIVERSAL SOCIAL PROTECTION

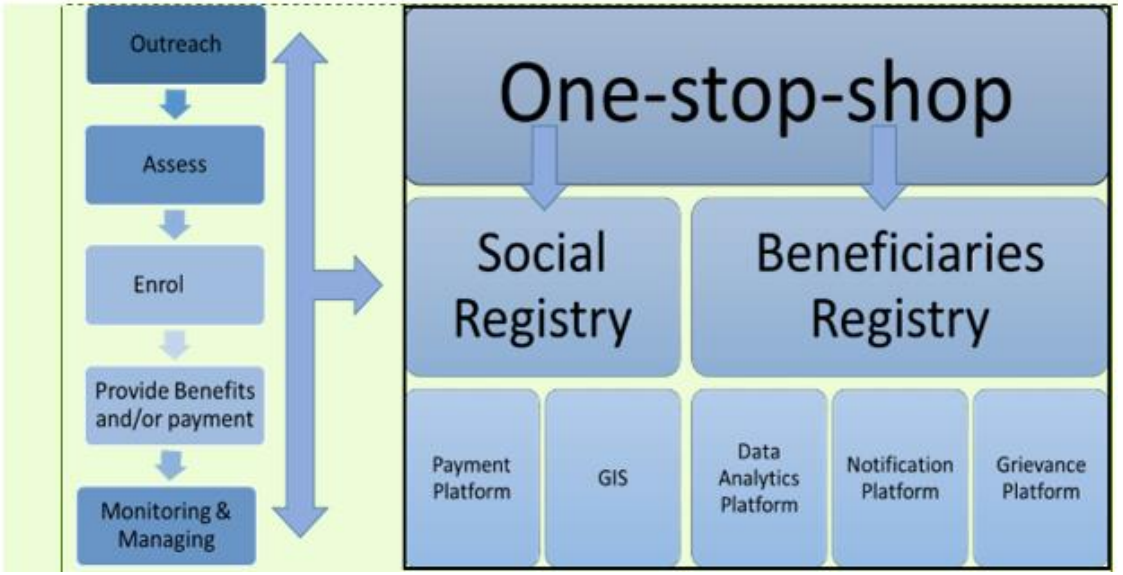
SPIAC - B

Components and their interactions



Sources: Tina George Karippacheril, Anita Mittal, consultant, Social Protection and Jobs, World Bank; Inés Rodríguez Caillava; and Kenichi Nishikawa Chávez; with inputs from Valentina Barca, consultant, GIZ and DFID.

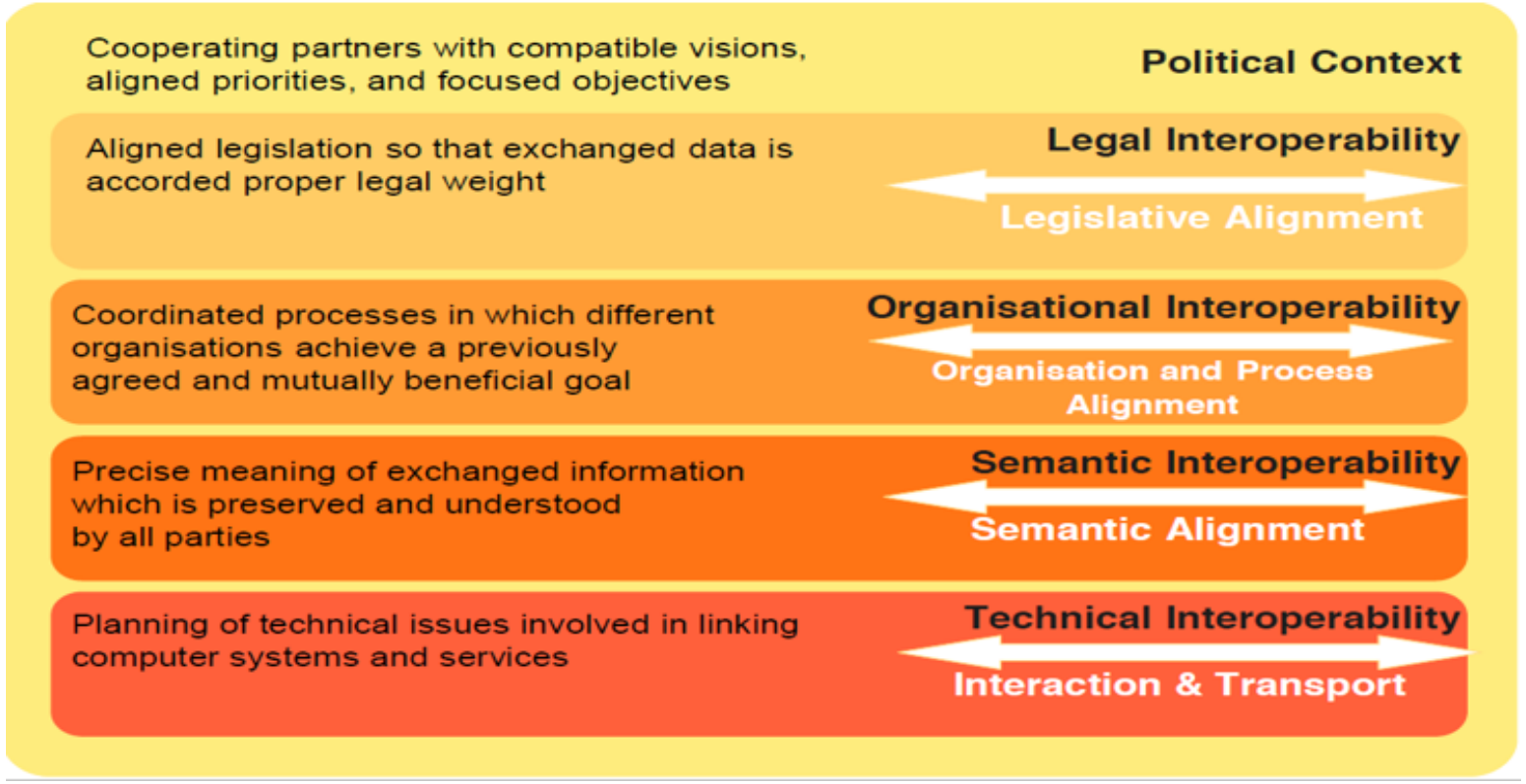
Figure 2. *Business components in Social Protection programmes*



4. Eligibility & Enrolment Decisions	Social Registry	Call Social Registry for read	read web service SOAP or REST preferably synchronous
		shared Social Registry data services	read asynchronous
	Social Security Registry	Call Social Security Registry for insert and update	update synchronous or asynchronous
		data exchange for update Social Security Registry	update asynchronous
	Health, Education	Call Health and Education Registry for read	web service SOAP or REST preferably synchronous and responsive
		replicated data	read
	Data analytics platform	data exchange for update Data analytics platform	update asynchronous

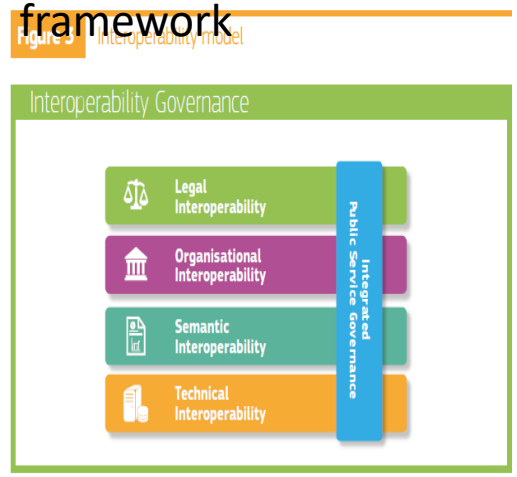
(405) New European Interoperability Framework - YouTube

INTEROPERABILITY SPANS SEVERAL LEVELS



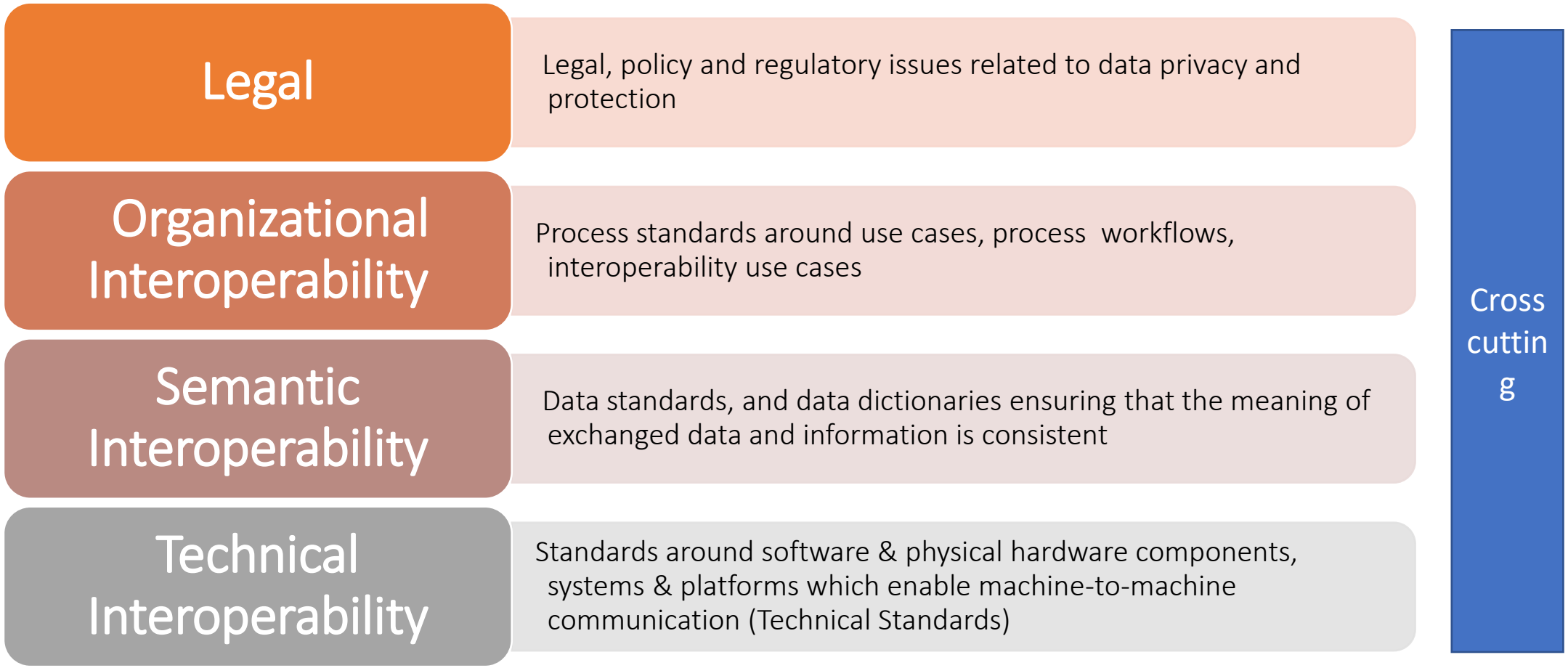
The Interoperability Frameworks, such as the European, the Estonian (and the US-SEI comprise these dimensions, often focusing on the Legal, Organizational, Semantic and Technical interoperability.

EU interoperability framework



Source : ISSA SP interoperability guidelines , Mariana Grunfeld and Raul Ruggia-Frick

Interoperability Framework– standards needed across all layers to develop interoperable Systems



Path to convergence

Phase I (Sep 2021 – Dec 2021)

- Establish a set of drafting groups to start building artefacts to address most common high-priority needs
- Understand the breadth of needs at the country-level to develop a long-term roadmap
- Map guidance that already exists to meet country-level needs

2022+

- Refine and finalize artefacts built during Phase I based on the review process
- Expand the artefacts to cover new processes, use cases and problems
- Test the artefacts in reference implementations before they can be adopted as standards
- Bring in standards development organizations for the accreditation of standards
- Develop a maturity model to help countries and programs adopt the standards
- Training and dissemination for wider adoption

PHASE 1 WILL FOCUS ON THE FOLLOWING ARTEFACTS

Starting with foundational artefacts that are perceived to be high priority in most countries – tell us if these are the right ones! As the initiative is being implemented in an agile mode, listing and prioritizing will be responsive to collective feedback

Legal (data protection)

- Data protection

Organizational (Processes)

- Process architecture (overall components across different program types)
- Process deep-dives (e.g., registration, payments)
  - Define minimum standards and best practices for workflow design and functional requirements
  - Define interoperability scenarios/use cases

Semantic (Data Standards, metadata)

- Data dictionary
- Data management and data governance

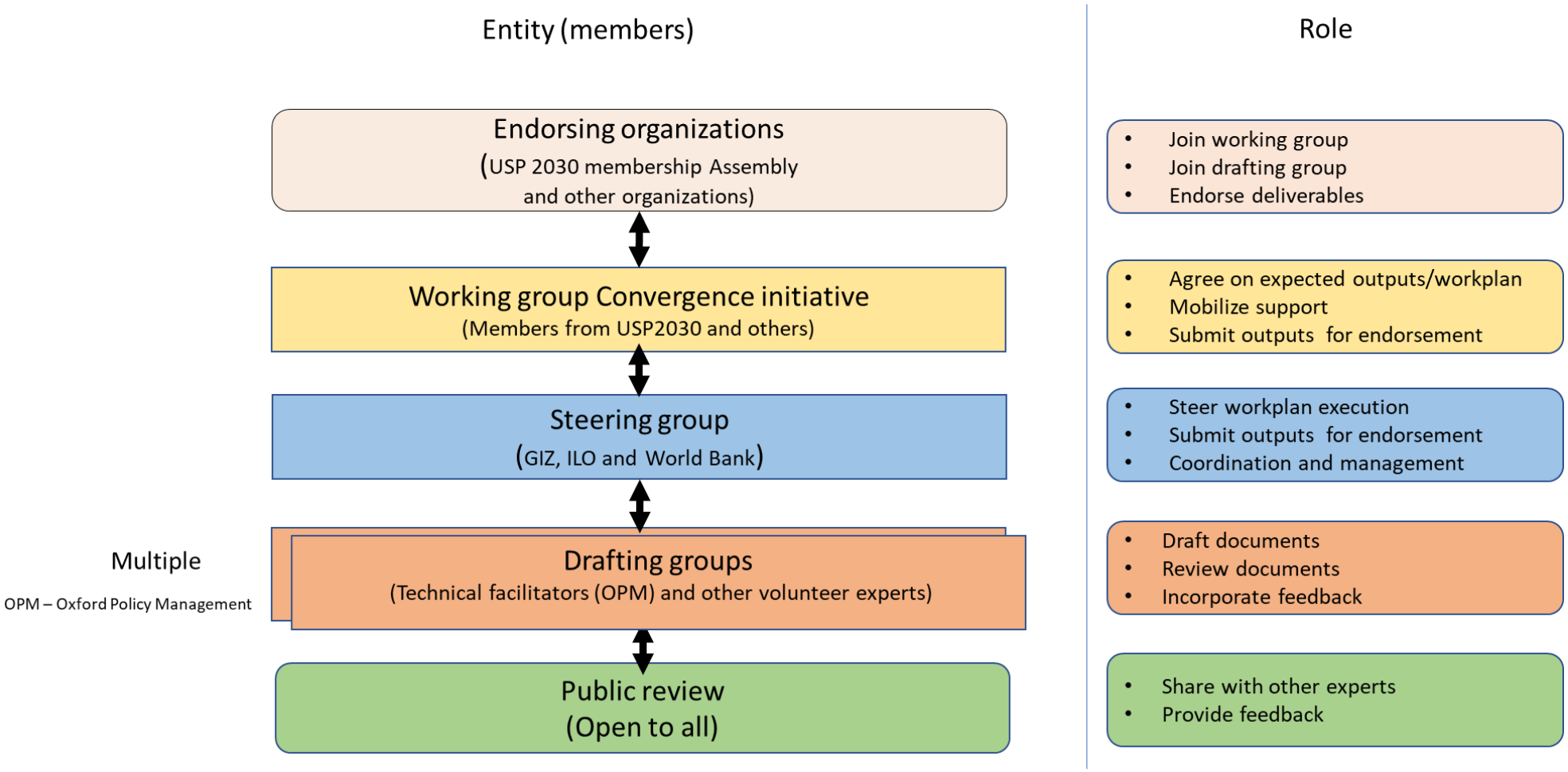
Technical standards

- API's /web services
- Technical standards e.g., biometric, digital signature, encryption

Cross cutting

- Principles to guide the development of digital solutions

COLLABORATION STRUCTURE



- ✓ **Support** the process of **consensus building and harmonization of standards**.
- ✓ **Spread awareness** about the initiative
- ✓ **Promote** adoption of **standards and other outputs**
- ✓ **Adopt the standards and other outputs** in your SP projects and share **feedback**

Participate in Phase 1 (Sept-Dec 21) in Drafting Groups

Group 1 : Principles
Group 2 : Process standards
Group 3 : Data standards
Group 4 : Technical Standards

Levels of participation

Level 1: Share existing materials

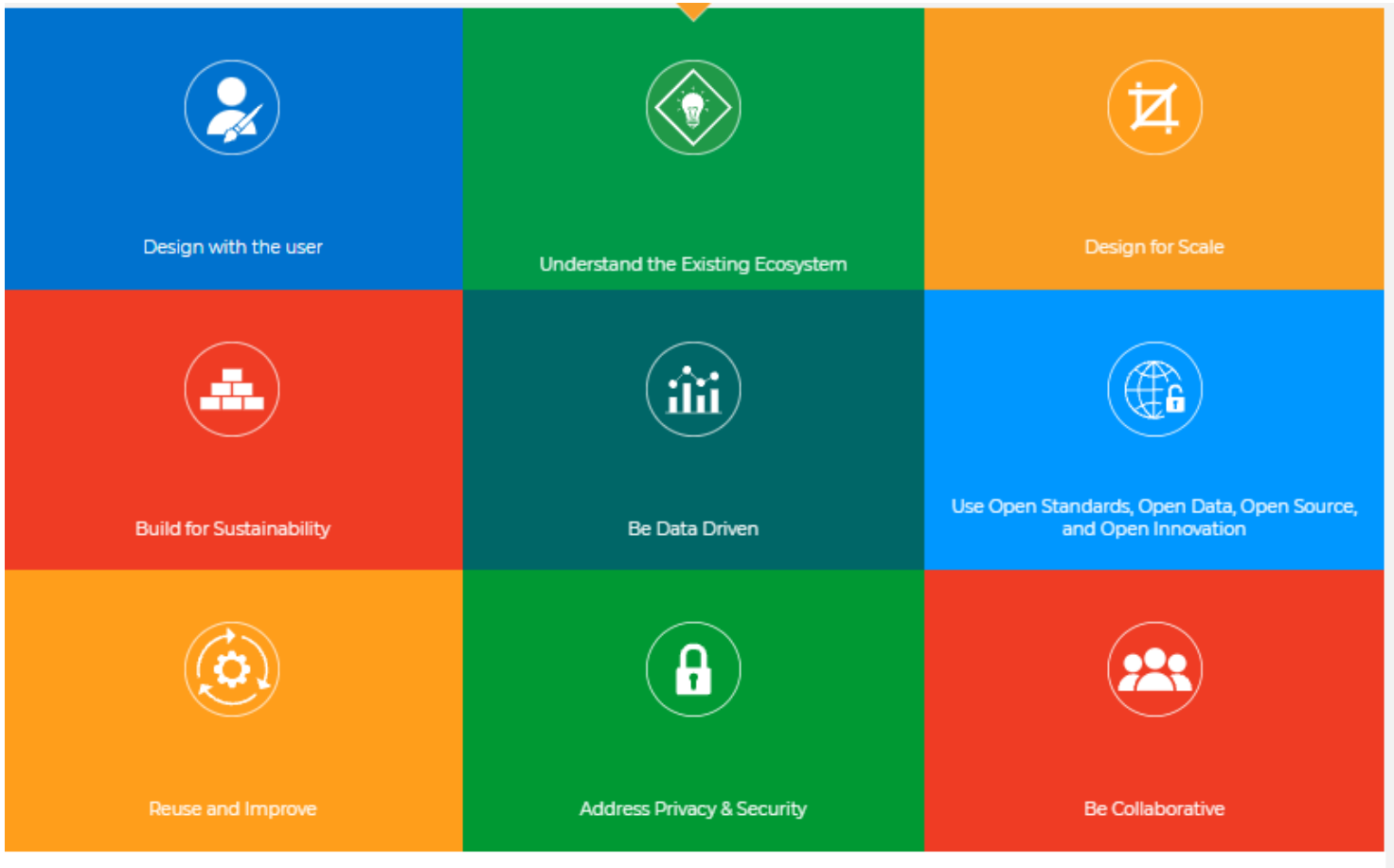
Level 2: Review outputs

Level 3: Join group discussions and validation workshops

Level 4: Drafting standards and guidelines alongside facilitators

Principles

- [Principles for Digital Development (digitalprinciples.org)]



Process standards

Interaction of systems for **registration**, eligibility assessment and enrolment

Interaction of systems for **payment**

Data Standards

Data standards as done in OpenHIE

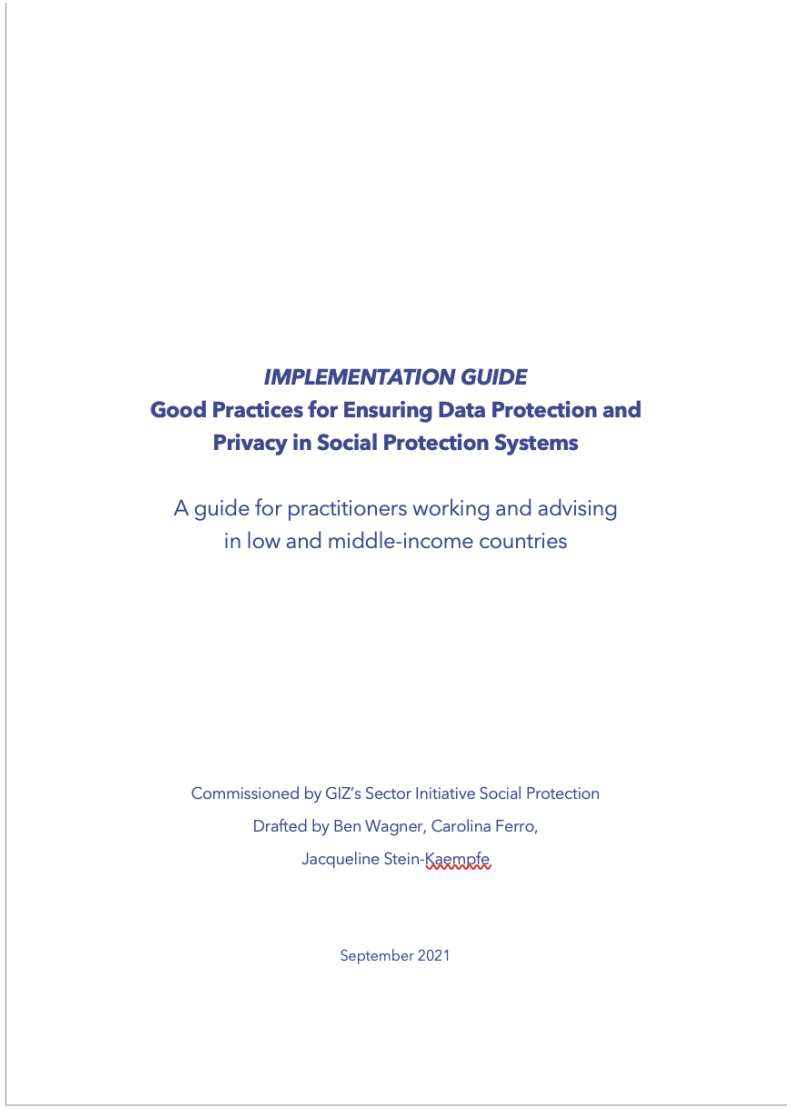
http://hl7.org/fhir/R4/datatypes.html#HumanName

http://hl7.org/fhir/R4/patient.html

workstream on data protection

How could data protection be implemented into SP programs?

- Journey started in 2020
- Long process to develop a guideline
- group discussions and validation workshops
- Review process
- It will be published in January.



IMPLEMENTATION GUIDE

Good Practices for Ensuring Data Protection and Privacy in Social Protection Systems

A guide for practitioners working and advising in low and middle-income countries

Commissioned by GIZ's Sector Initiative Social Protection

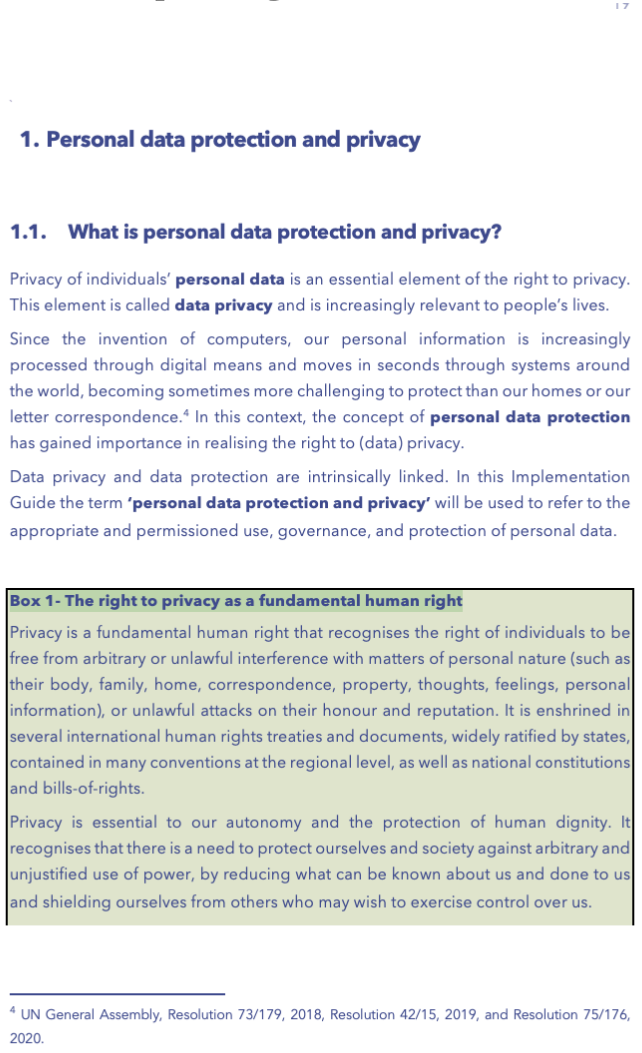
Drafted by Ben Wagner, Carolina Ferro, Jacqueline Stein-Kaempfe

September 2021

How could data protection implemented into SP programs?

PART I : Personal data protection and privacy

- What is personal data protection and privacy?
- International and regional data protection and privacy instruments
- Key terms you should know



1. Personal data protection and privacy

1.1. What is personal data protection and privacy?

Privacy of individuals' **personal data** is an essential element of the right to privacy. This element is called **data privacy** and is increasingly relevant to people's lives.

Since the invention of computers, our personal information is increasingly processed through digital means and moves in seconds through systems around the world, becoming sometimes more challenging to protect than our homes or our letter correspondence.[4] In this context, the concept of **personal data protection** has gained importance in realising the right to (data) privacy.

Data privacy and data protection are intrinsically linked. In this Implementation Guide the term **'personal data protection and privacy'** will be used to refer to the appropriate and permissioned use, governance, and protection of personal data.

Box 1- The right to privacy as a fundamental human right

Privacy is a fundamental human right that recognises the right of individuals to be free from arbitrary or unlawful interference with matters of personal nature (such as their body, family, home, correspondence, property, thoughts, feelings, personal information), or unlawful attacks on their honour and reputation. It is enshrined in several international human rights treaties and documents, widely ratified by states, contained in many conventions at the regional level, as well as national constitutions and bills-of-rights.

Privacy is essential to our autonomy and the protection of human dignity. It recognises that there is a need to protect ourselves and society against arbitrary and unjustified use of power, by reducing what can be known about us and done to us and shielding ourselves from others who may wish to exercise control over us.

[4] UN General Assembly, Resolution 73/179, 2018, Resolution 42/15, 2019, and Resolution 75/176, 2020.

How could data protection implemented into SP programs?

PART II: Why is personal data protection critical for social protection programmes?

- Social protection and personal data
- Why is data protection needed in social protection?
- Main stakeholders and responsibilities
- Digital technologies increase the urgency of data protection
- There is no contradiction between the right to (data) privacy and the right to social protection

25

2. Why is personal data protection critical for social protection programmes?

2.1. Social protection and personal data

Social protection has slightly different meanings for different institutions. For example, the SPIAC-B defines social protection as:

> "Social protection encompasses the set of policies and programmes aimed at preventing or protecting all people against poverty, vulnerability and social exclusion, throughout the lifecycle, with a particular emphasis on vulnerable groups. Social protection includes social assistance, social insurance, and labour market interventions. It can be provided in cash or in-kind, through non-contributory and contributory schemes, and by building human capital, productive assets, and access to jobs."[9]

Furthermore, social protection is a human right,[10] and social protection programmes and policies support individuals and societies with risk management. Therefore, social protection programmes include instruments to improve resilience, equity and opportunity.[11] Social protection interventions include various types, such as categorical programs for child allowances or social pensions, conditional and unconditional cash transfers, unemployment and disability assistance and insurance, active labour market programs, employment services, training services, social and social work services.[12] These components vary from country to country, and programmes are often government-owned. Social protection programmes usually target poor, marginalised or vulnerable groups to increase the presence and effectiveness of safety nets.[13] However, depending on the programme, different population groups are intended, like children, the elderly, low-income families, the

[9] SPIAC-Bb, n.d.
[10] United Nations 2015 (Art. 23 and 25).
[11] Leite et al. 2017 (p. 96).
[12] Lindert et al. 2020 (p. 2).
[13] WFP 2017.

How could data protection implemented into SP programs?

PART III Good international practice of data protection and privacy

- 1. Data protection and privacy standards
- 2. Data processing principles
- 3. Data subject rights
- 4. Accountability, oversight and enforcement
- 5. International data sharing
- 6. Sensitive personal data

How could data protection implemented into SP programs?

Principles

Data protection works through a set of **guiding principles** related to the processing of personal data.

They are interrelated and overlap. It is essential to treat them together, as a whole.

Individual's data rights

What are the main rights to be considered?

1. Right to information
2. Right to access
3. Rights to rectify and erasure
4. Right to object
5. Right to data portability
6. Rights related to profiling and automated decision making
7. Right to an effective remedy
8. Right to compensation and liability

How could data protection implemented into SP programs?

PART IV: How to implement data protection and privacy into social protection programmes?

- 1. How to promote and adopt standards for data protection and privacy?
- 2. How to conduct a data protection impact assessment (DPIA) and ensure privacy by design?
- 3. How to apply the data protection and privacy standards to social protection programmes?
- 4. How to work with providers of digital technologies?

Box 27 - Checklist of Good Practices: Lawfulness, fairness, and transparency principle

- ☐ Determine the legal basis for each processing activity relating to a specific purpose
- ☐ Obtain and process personal data with a lawful basis, fairly and in a transparent manner
- ☐ Ensure transparent and fair information and communication with data subjects by clearly informing them, at the time of data collection, on how, why and when their personal data is being processed, both where they have provided this directly to a controller and where the controller has obtained it from another source
- ☐ Inform data subjects about their data rights
- ☐ Guarantee that any information and communication relating to the processing of personal data is easily accessible, legible, understandable, and adapted to the relevant data subjects.
- ☐ Ensure that the data subjects' consent is informed, freely given and specific. In the case of processing sensitive personal data, consent should also be explicit. It should be possible to withdraw consent at any time. Any exceptions where obtaining consent is not possible should be very limited, requiring heightened levels of transparency, only applied on an individual case-by-case basis, and another legal and legitimate basis for personal data processing is required.
- ☐ Offer data subjects alternatives that will allow them to continue receiving assistance should they not provide or object to the programme's processing of their personal data, especially in the case of sensitive personal data.

How could data protection implemented into SP programs?

PART V: Boxes

- Definitions and explanations
- Checklist of good practices
- Implementation tools
- Examples

Box 6 - Legal bases for processing personal data

According to the international and regional data protection and privacy frameworks, the legal bases for processing personal data may include the following.[45] The processing shall be lawful only if and to the extent that at least one of them applies:

1) Public interest: Public interest is the appropriate legal basis when the processing of personal data is necessary to exercise official authority or a task in the public interest and the task has a basis in law. Public interest grounds could be the administration of justice, public health and social security, the prevention, investigation, detection and prosecution of criminal offences, and the execution of criminal penalties, the enforcement of civil law claims, among others. For international organisations, the legal basis of public interest applies when the activity in question is part of a humanitarian mandate established under national or international law or is otherwise an activity in the public interest laid down by law.[46]

2) Vital interests: The processing is necessary to protect the vital interests of a data subject or another person (i.e., protect someone's life, integrity, health, dignity, or security). In the case of vital interest, it is necessary that this legal basis is accompanied by sufficient elements to consider that, in the absence of the personal data processing, the individual could be at risk of physical or moral harm.

3) Legal obligation: The processing is necessary for compliance with a legal obligation to which the controller is subject (not including contractual obligations). It is not necessary that this legal basis expressly permits specific data processing activities, such as data collection. For example, a social protection law may oblige a specific domestic authority to provide assistance to applicants which provide evidence of being under a poverty level. In this case, the authority is required to collect the data to assess those conditions and to ensure delivery of the benefits to the targeted persons, to comply with its legal obligation.

4) Informed consent: Consent indicates the data subjects' agreement to the processing of personal data relating to them for a specific purpose. Where the processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to the processing of his or her personal data. If the data subject does not provide consent, the data cannot be processed on this legal basis. Consent won't always be the most appropriate legal basis.

connect & engage with the convergence initiative

How to participate?

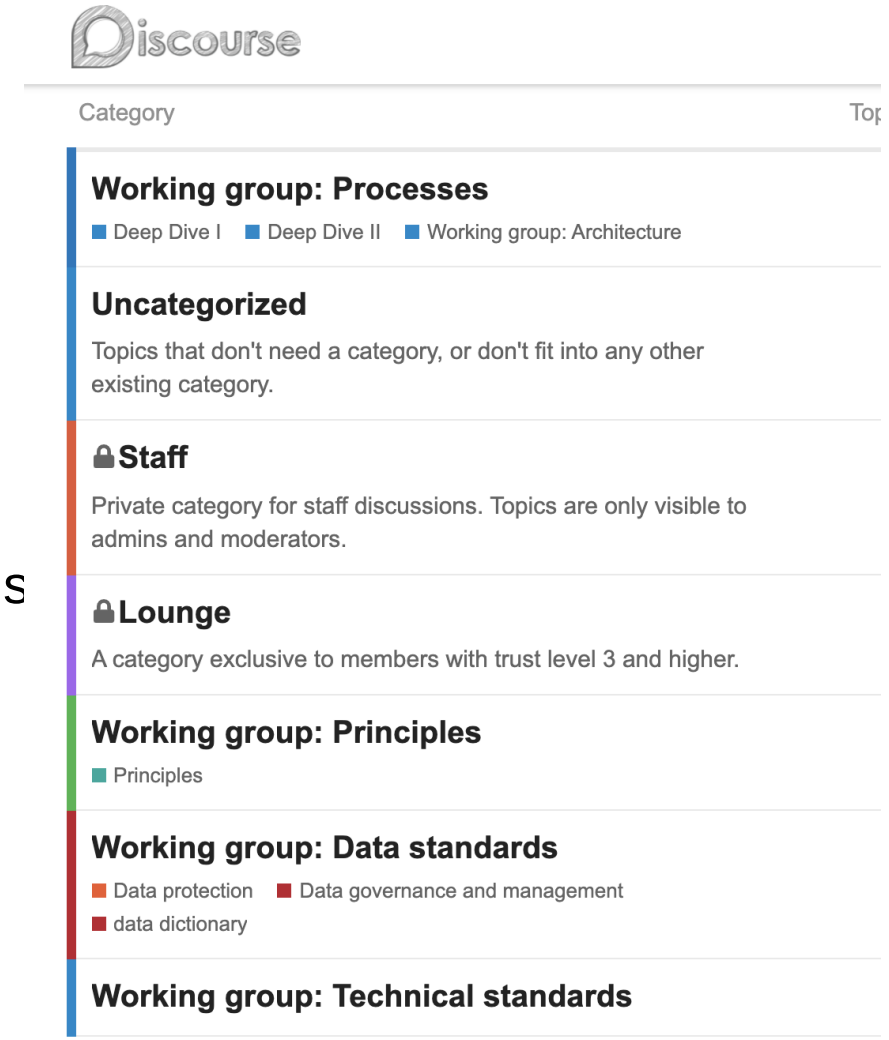
- Formular online
- Email

Which of the following groups would you like to join?

- Principles, Process standards, Data standards, Technology s

How would you like to participate?

- Level 1: Share existing materials
- Level 2: Review outputs
- Level 3: Join group discussions and validation workshops
- Level 4: Drafting standards and guidelines alongside facilitators



How to engage?

- **Support** the process of **consensus building and harmonization of standards**.
- **Spread awareness** about the initiative
- **Promote** adoption of **standards and other outputs**
- **Adopt the standards and other outputs** in your SP projects and share **feedback**

Communication channels

Email

mail@sp-convergence.org

Website

https://sp-convergence.org

Linked In

LinkedIn

https://www.linkedin.com/company/social-protection-convergence-initiative

Discussion forum

Discourse

https://socialprotection-convergence.discourse.group/

Twitter

@sp_convergence

Instagram:

@sp_convergence