



Findings use case
Monitoring Human Trafficking

Table of contents

1. Management summary

2. Use case description
3. Appendix
 - A. Proof of concept description
 - B. Introduction to multi-party computation
 - C. Overview of organisations monitoring human trafficking
 - D. DSC use case support
 - E. Organisations involved in the use case

Management Summary

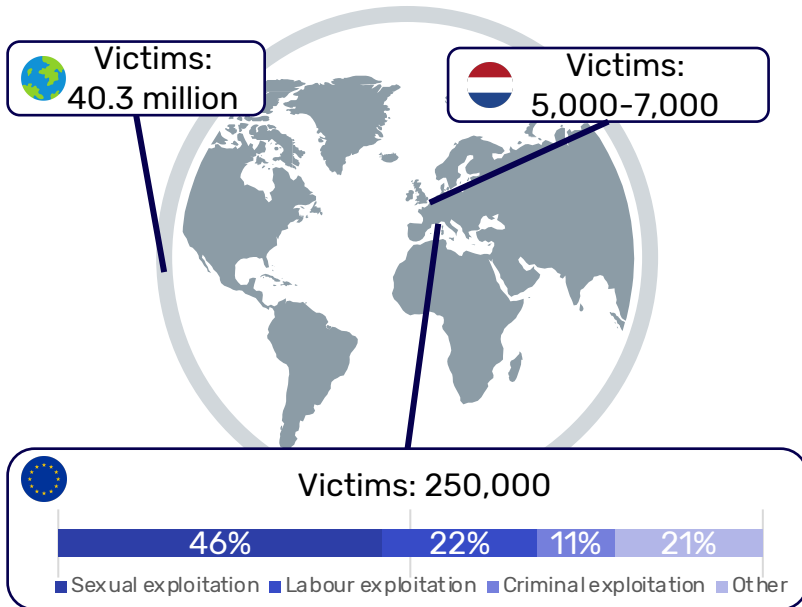
1. A global estimate of over 40 million people are victims of the crime of human trafficking
2. Combatting human trafficking is limited by the lack of data collaboration due to legal and trust barriers
3. Multi-party computation (MPC) can reduce barriers in data collaboration as sensitive source data is not revealed
4. For this DSC use case, a scalable design for MPC-based data collaboration was created that enables organisations to improve the monitoring of sexual exploitation
5. Data collaboration characteristics of this use case design include data sensitivity, organisational diversity and the use of MPC as privacy-enhancing technology
6. Legal and technical privacy measures, governance and education have been identified as key enablers to realise value in this use case
7. Based on the success of this use case, a Sandbox is the next step towards realising the ambition of a data space for monitoring sexual exploitation
8. After initial setup, the data space can be scaled to further improve the data collaboration for monitoring human trafficking
9. Connecting different MPC-based data spaces optimally captures the value from secure data collaboration

Table of contents

1. Management summary
- 2. Use case description**
3. Appendix
 - A. Proof of concept description
 - B. Introduction to multi-party computation
 - C. Overview of organisations monitoring human trafficking
 - D. DSC use case support
 - E. Organisations involved in the use case

A global estimate of over 40 million people are victims of the crime of human trafficking

Estimated number human trafficking victims



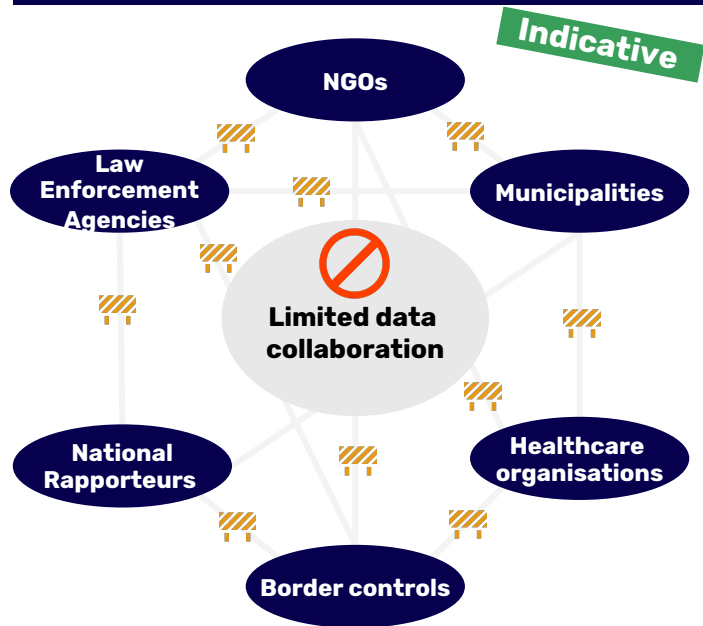
Estimated numbers are used as only a fraction of the actual number of victims is registered

Background on human trafficking and victims

- *Definition:* Human trafficking includes recruiting, transporting, receiving and housing human beings through the use of force, for the purpose of exploiting them
- Human trafficking is a growing global problem with many victims. The total profit being made by crime groups is estimated at 150 billion US\$.
- There are various kinds of human trafficking, including:
 - **Sexual exploitation:** a person is forced to have sex in return for money, clothes or food, which must be turned over to the exploiter
 - **Labour exploitation:** a worker is forced to hand over income or is forced to work in inhumane conditions
 - **Criminal exploitation:** a person is forced to beg, steal or engage in other criminal activities, and hand over the goods or money to the exploiter

Combatting human trafficking is limited by the lack of data collaboration due to legal and trust barriers

Limited data collaboration



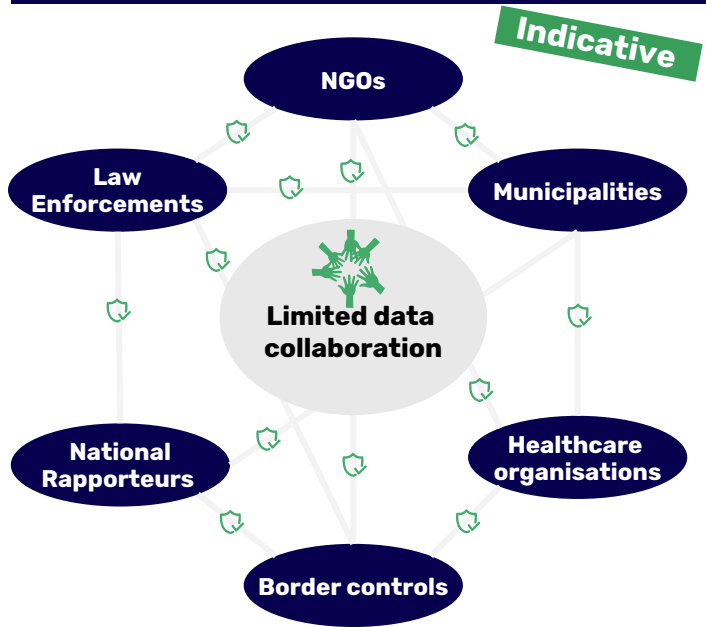
- Organisation with fragmented data
- Legal and trust barriers

Combatting human trafficking requires data collaboration

- Human trafficking is a profitable business for crime groups. The European Commission has set out a strategy for 2021-2025 to combat criminal groups. A key objective is to make human trafficking a high-risk, low-return crime by lowering the potential profits and increasing the risk of prosecutions.
- The ability to monitor human trafficking is essential for making it a high-risk crime as detailed insight into the activities of victims and traffickers allows public institutions to dismantle the crime groups
- Large scale data collaboration is required for the monitoring of human trafficking as many different organisations are involved in monitoring human trafficking and all need detailed insights
- Barriers limiting data collaboration include:
 - Legal complexity** in sharing data based on the personal identifiable information (PII) in the data
 - Lack of trust** due to the different perspectives of collaborating organisations, from victim-centric to offender-centric

Multi-party computation (MPC) can reduce barriers in data collaboration as sensitive source data is not revealed

MPC-secured data collaboration



● Organisation with fragmented data
🛡️ Data collaboration secured by MPC

Introduction to multi-party computation (MPC)

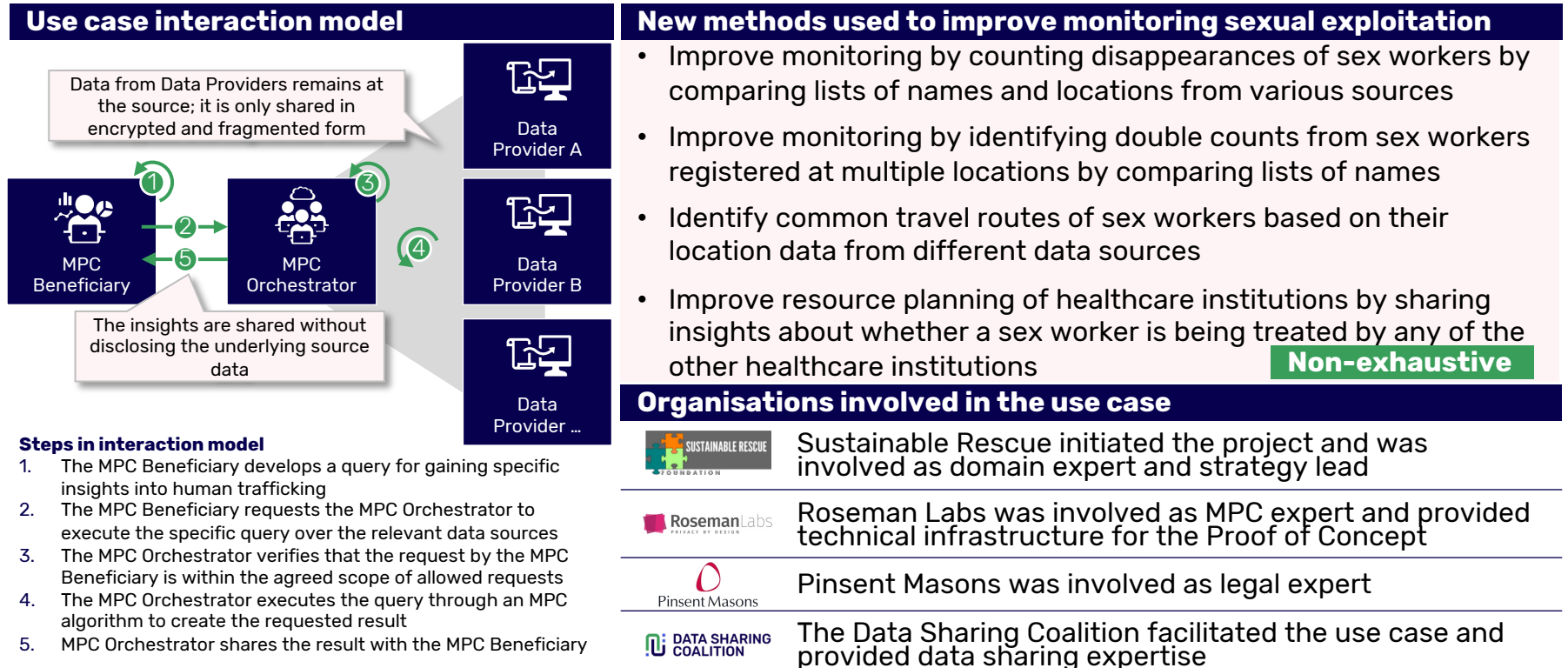
- Multi-party computation (MPC) allows different organisations to jointly create insights from data without any individual organisation revealing their source data to other organisations involved
- Source data from individual organisations is secured by fragmenting and encrypting it before providing it to MPC. This means that each organisation retains control over their own data
- MPC creates the insights by performing calculations on fragmented and encrypted data from different organisations

Impact of MPC on data collaboration barriers

- **Legal complexity:** MPC-based data collaboration reduces the legal barrier of *sharing* data, as no PII is shared. Organisations still need to *process* PII. Monitoring the legal context of multi-party computation is key as it is still in development.
- **Lack of trust:** MPC-based data collaboration facilitates the necessary trust between organisations as no PII is shared

[See Appendix for PoC description and MPC introduction](#)

For this DSC use case, a scalable design was created for MPC-based data collaboration for monitoring sexual exploitation



Data collaboration characteristics of this use case design include data sensitivity, organisational diversity and the use of MPC

Key characteristics of the data collaboration context of this use case

Non-exhaustive



Data sensitivity

The data used for collaboration includes personal identifiable information (PII) of people who are possibly victims of human trafficking. Additionally, crime groups may retaliate against victims if they find out they are in contact with aid workers.



Diversity of organisations combatting human trafficking

Many organisations in the public, civil and private sectors are involved in the monitoring of human trafficking but they have different goals. For example, law enforcement focuses on criminal interventions whereas care takers focus on the victims. Different goals mean that organisations need to maintain control over which organisations to collaborate with and what data to share.



Use of multi-party computation

MPC-based data collaboration is an innovative concept. Awareness about the possibilities with MPC is low at most organisations. Increasing the awareness of MPC is key to realise the potential of MPC-based data collaboration as new applications of the insights will be developed.

Data collaboration context

- Every data sharing use case has its own data context. This context is determined by factors such as the nature of the data that is shared, the actors that are involved, who controls the data, et cetera.
- This data collaboration context is very relevant, as it influences the requirements for the use case design

Legal and technical privacy measures, governance and education have been identified as key enablers to realise this use case

Key characteristics



Data sensitivity



Diversity of organisations



Use of MPC

Enablers for data collaboration as identified in this DSC use case



Legal and technical privacy measures

The secure handling of sensitive data is ensured by the use of privacy measures such as Data Protection Impact Assessments, multi-party computation, access controls, data retention policies and data minimisation policies



Governance

To enable the trust in the data collaboration between a variety of organisations, governance of the data collaboration environment is essential. All actors should be able to provide input for the development of the data collaboration environment to make sure it aligns with their needs




Support & Education

To raise the awareness of and trust in secure data collaboration, support and education about MPC are needed. This can include onboarding materials, demonstrations of the technology, sandbox environments and easily available user support

A sandbox is the next step for this use case to realise the ambition to set-up a monitoring sexual exploitation data space

Roadmap for realising the ambition

	PoC 	Sandbox	Data space
Use cases	1	5	N
Involved organisations	3	±7	±30
Organisation of trust	Trust MPC and Roseman Labs hardware	Trust in consortium	Trust between organisations is organised in scheme
Technical implementation	Roseman Labs laptops at locations	Online portal in webbrowser	Online portal and on-site implementation
Legal context	One-time contract	Overarching legal framework	Overarching legal framework
Availability of data in network	One-time availability	Continuous availability	Continuous availability

Description of data space ambition

- The data space is a digital environment for all organisations involved in monitoring sexual exploitation. Source data is protected and always under the control of the Data Provider
- The data space intends to connect ±30 different organisations as Data Providers and MPC Beneficiaries
- This roadmap for the realisation of the data space shows the necessary infrastructure and agreements and key topics

Join the Sandbox

- The Sandbox is open for any organisation interested in monitoring human trafficking
- To join the Sandbox, please contact paul.fockens@sustainerescue.com

After initial setup, the data space can be scaled to further improve the data collaboration for monitoring human trafficking

Data space scaling options

Monitoring sexual exploitation in the Netherlands

Monitoring human trafficking in general



More organisations

More data

More queries

More countries

More types of exploitation

New organisations can participate in the data space. See Appendix for overview of involved organisations in NL

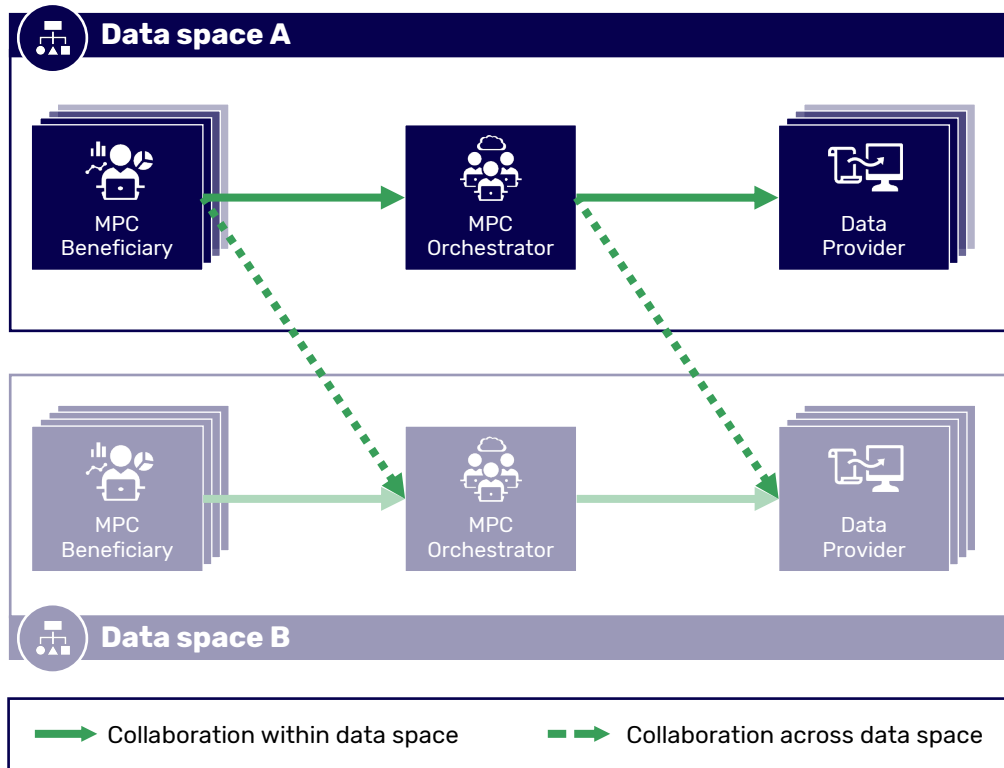
Organisations can increase the data they make available for MPC queries. An organisation can enrich current data or increase the scope of currently available data

More queries can be developed based on the experience from the data space. The insights from the new queries help to further improve the monitoring

Organisations from other countries can be included in the data space as human trafficking is a global issue

Additional types of exploitation can be included (e.g. criminal exploitation) based on stakeholder needs

Enabling data space participants to collaborate with other data spaces optimally captures the benefits of data collaboration



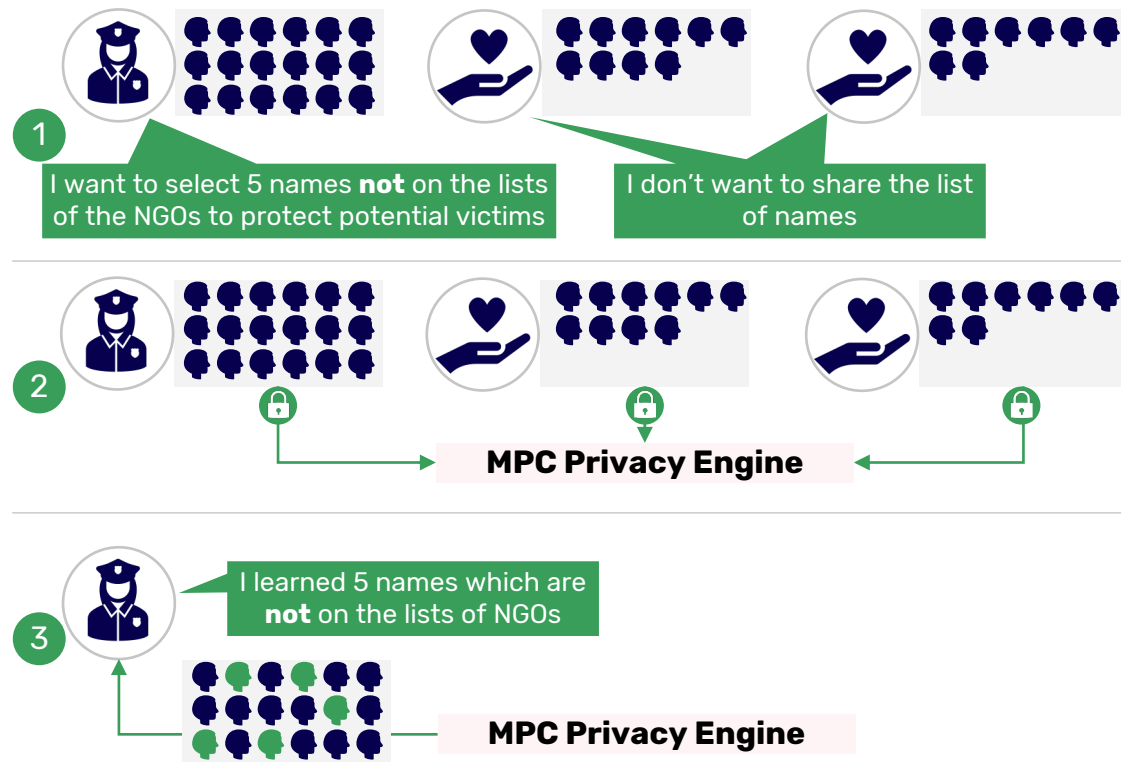
Description

- Enabling participants from one data space to collaborate with participants in other data spaces optimally captures the value from secure data collaboration
- In order to realise this cross data space collaboration, three key topics are identified:
 - **Standardised Data Provider modules** to ensure a Data Provider only needs one module for secure data collaboration in different data spaces
 - **Enrolment process** which ensures that new participants/use cases are aligned with all participants in the data space
 - **Fine-grained consent mechanism** which ensures that Data Providers remain in control over their data. This mechanism must be included in the privacy engine of the MPC Orchestrator

Table of contents

1. Management summary
2. Use case description
- 3. Appendix**
 - A. Proof of concept description
 - B. Introduction to multi-party computation
 - C. Overview of organisations monitoring human trafficking
 - D. DSC use case support
 - E. Organisations involved in the use case

The successful execution of the PoC increased the awareness and trust of law enforcement agencies and NGOs in MPC

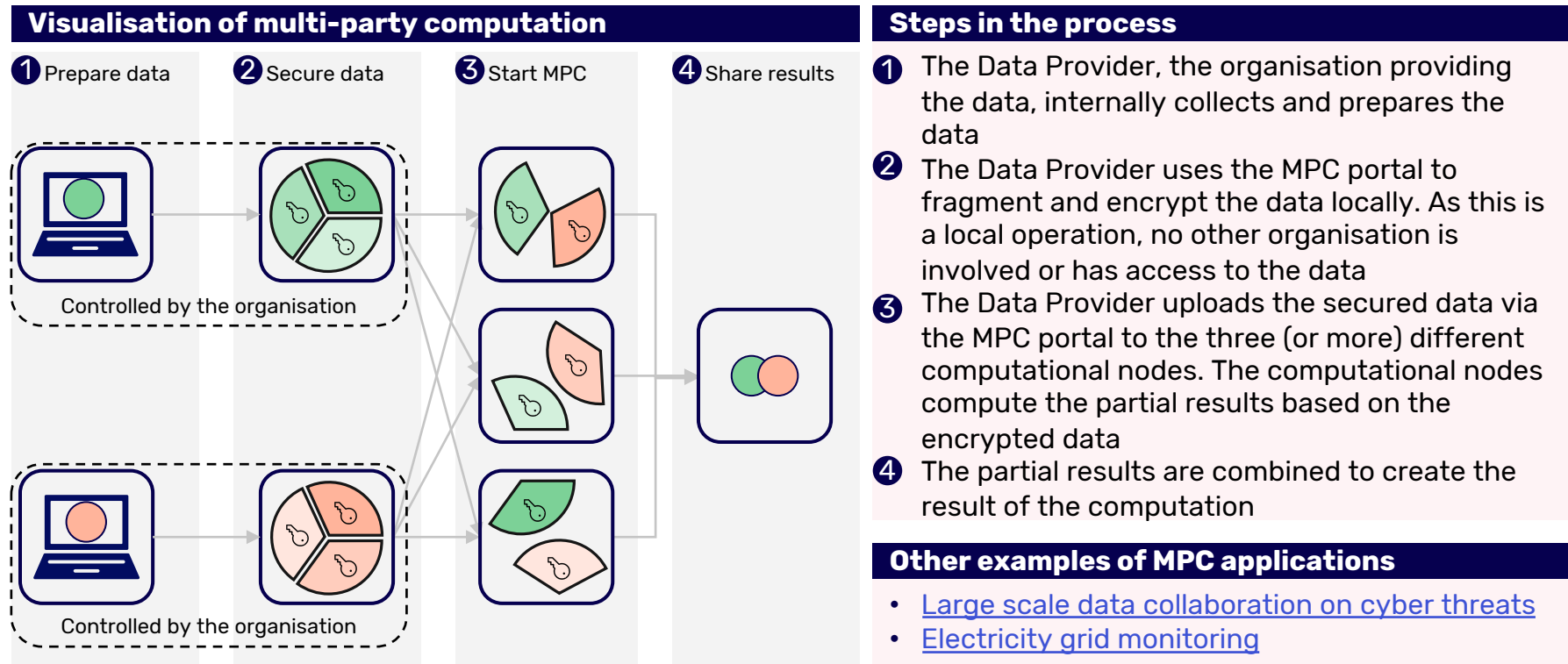


Explanation Proof of Concept

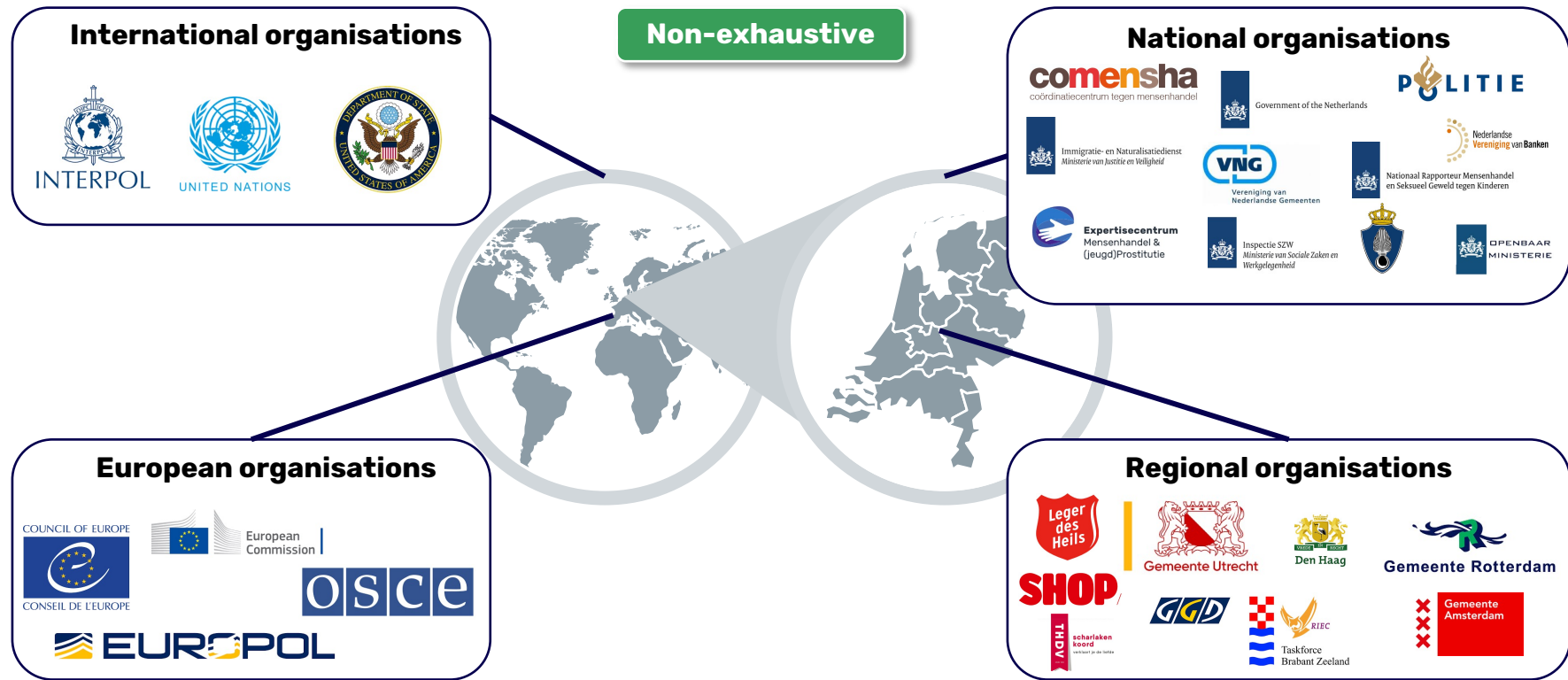
- 1 The Law enforcement agency (LEA) wants to select 5 names which are not on the lists of the NGOs. The LEA can not share their list due to regulation. The NGOs will not share theirs as they fear to break the trust relationship with their informants
- 2 The LEA and NGOs use the MPC Privacy Engine to jointly perform the comparison without disclosing any individual's name
- 3 The LEA learns 5 names which are not on the lists of NGOs

- Law enforcement agency
- Name on list of NGO or LEA
- NGO
- Name not on list NGO
- Shared in encrypted and fragmented way

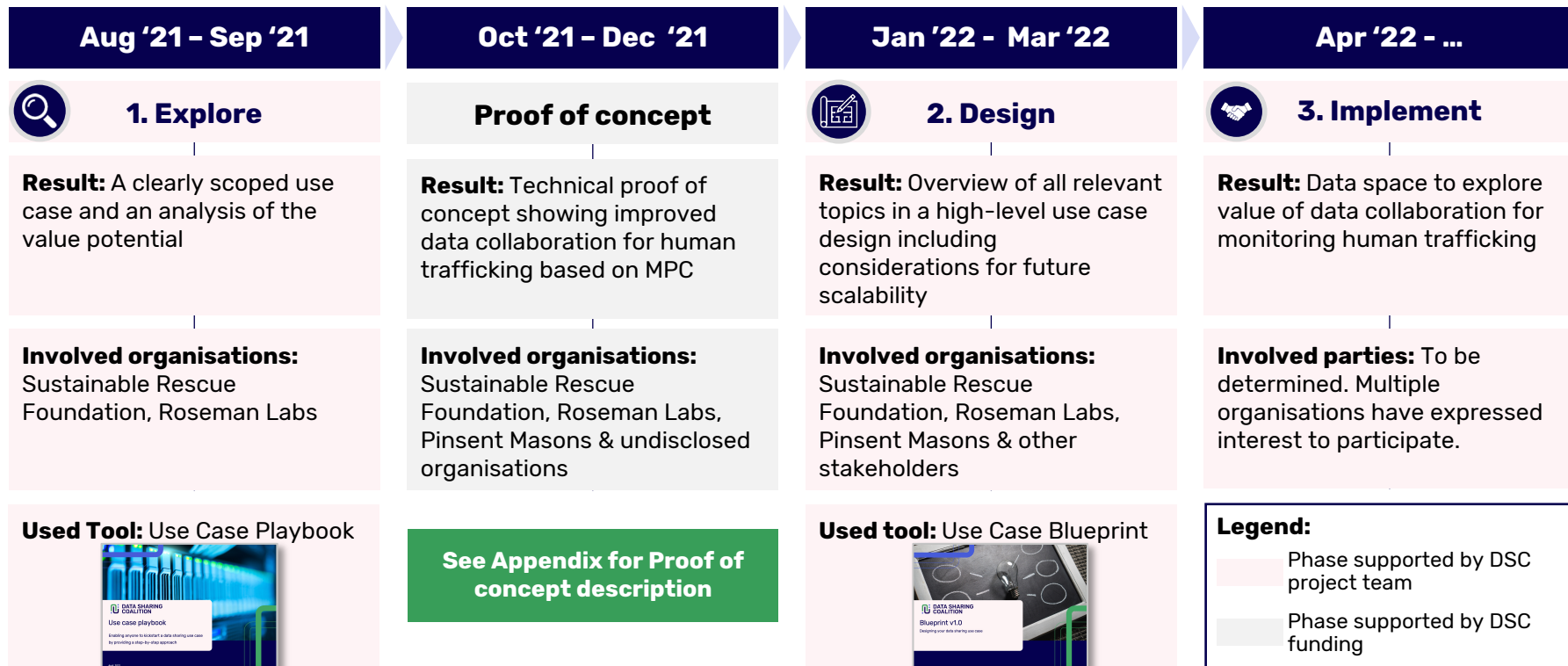
MPC enables a group of organisations to calculate certain insights without sharing individual organisation's data



Organisations involved in monitoring human trafficking operate at international, national and regional levels



From August 2021 to March 2022, we worked towards a use case scope, Proof of Concept and use case design



Sustainable Rescue Foundation and Roseman Labs initiated the use case, Pinsent Masons was involved for the legal expertise



- [Sustainable Rescue Foundation](#)'s aims to develop an ecosystem to fight human trafficking
- It focuses on integrating existing business best practices, digital technology, academic concepts, and legislation to facilitate collaborative work environments
- SRF initiated the use case and ensured the alignment of the use case with NGOs and public authorities



- [Roseman Labs](#) (RL) is a high-tech software company with the mission of transforming how organisations collaborate on sensitive data with robust privacy
- RL specialises in deploying high performance MPC solutions
- RL delivered the software and privacy engine for the PoC and the use case design is based on their architecture



- [Pinsent Masons](#) (PM) is an international law firm
- PM's department that was involved in the use case specialises in data protection and privacy
- In the use case, PM provided legal expertise related to MPC-based data collaboration

Other organisations involved in monitoring human trafficking were involved to ensure that the use case aligned with their needs.