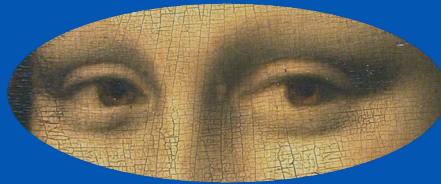




The JOCONDE Project at Eurostat

Joint On-demand Computation with No Data Exchange



Fabio Ricciato

Eurostat, Unit A.5 Methodology and Innovation in official statistics

Global PETs Network Meeting

21 January 2025

Eurostat

European Statistical System (ESS)



- The ESS is a **partnership** between statistical organisations
 - Independency
 - Collaboration
 - Governance

Article 4

The European Statistical System

The European Statistical System (ESS) is the **partnership** between the Community statistical authority, which is the Commission (Eurostat), and the national statistical institutes (NSIs) and other national authorities responsible in each Member State for the development, production and dissemination of European statistics.

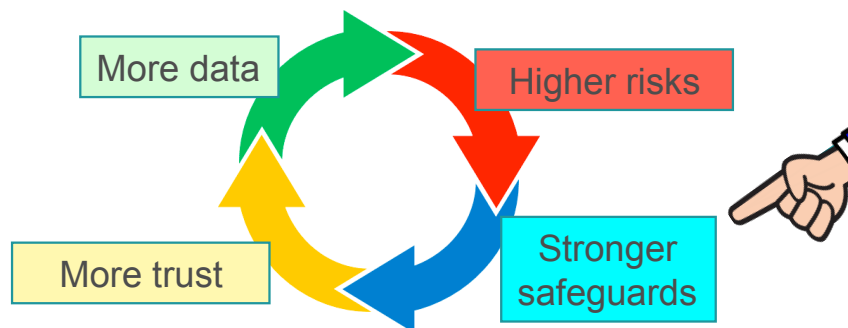
Regulation (EC) No 223/2009 on European statistics ([link](#))

Partnership(*)

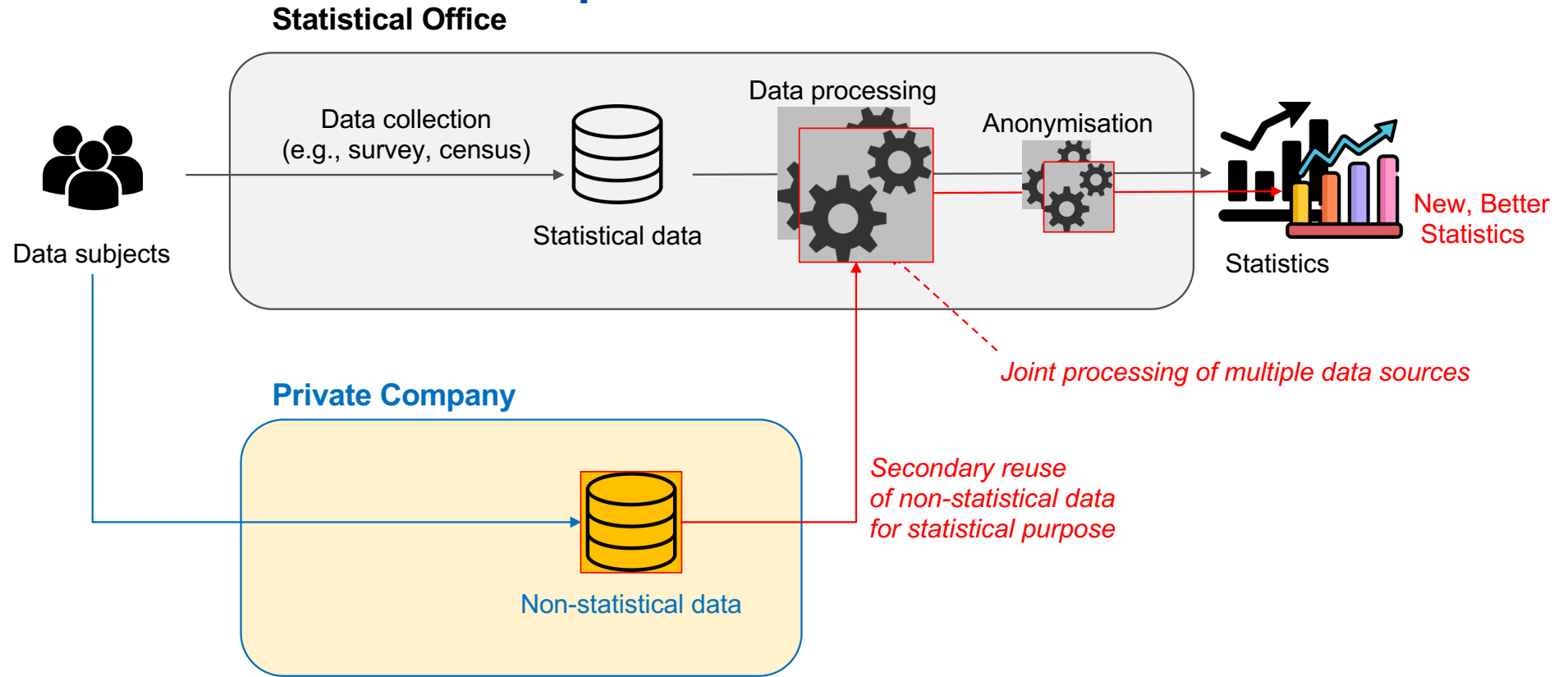
PET = Privacy Enhancing Technologies

Why caring? Context and drivers

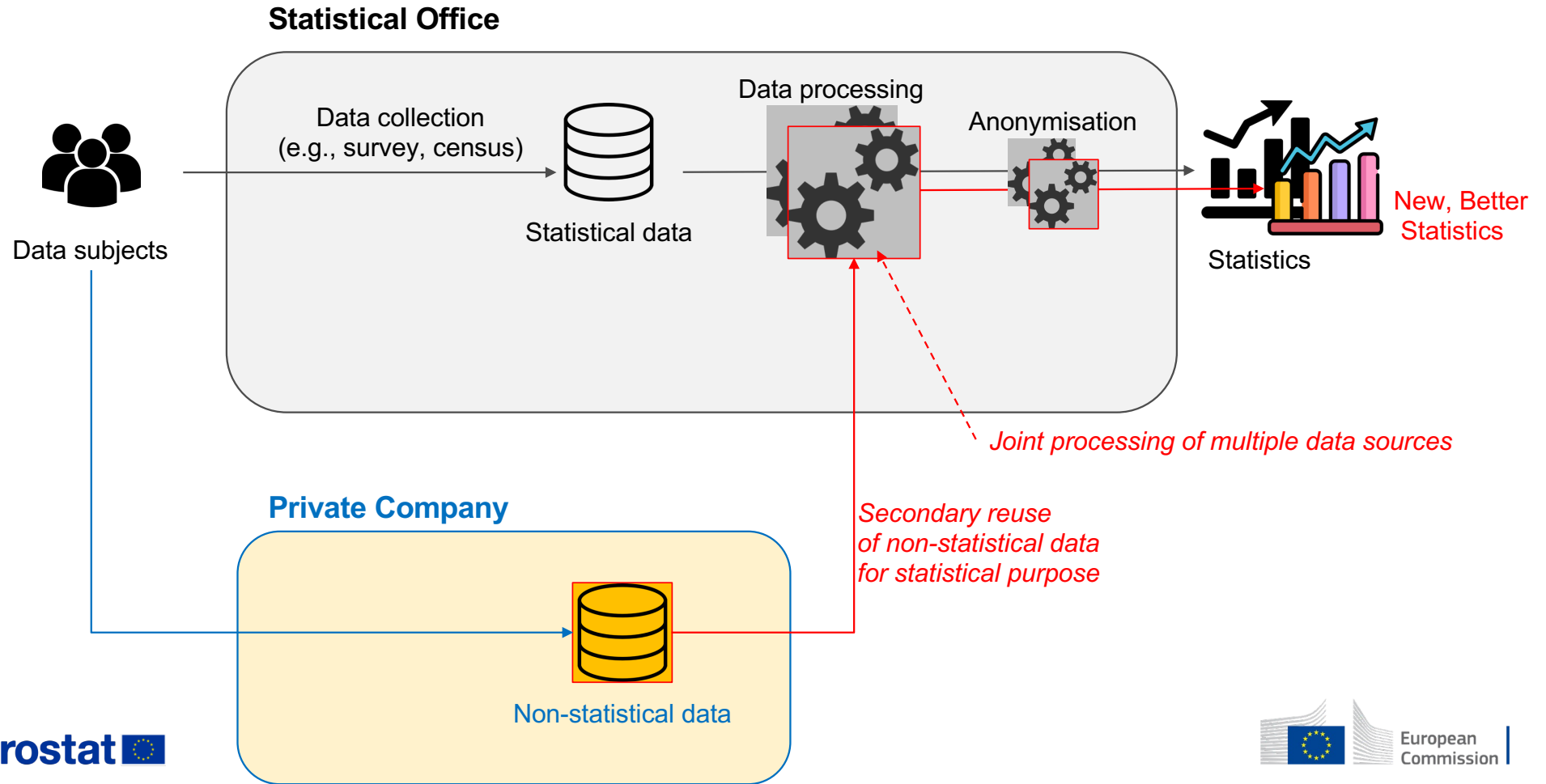
- Innovation trends in official statistics concur to increase the demand for **cross-organisational data processing**
 - Data held by **NSIs in different Member States** concerning cross-border phenomena (e.g., international trade, migration, ...)
 - Statistics based on data held by other **public bodies** (e.g., administrative records)
 - New statistics based on **privately held data**, requiring integration across different providers (e.g., Mobile Network Operators) and possibly with statistical data
- Increasing attention by the general public to **personal data protection**



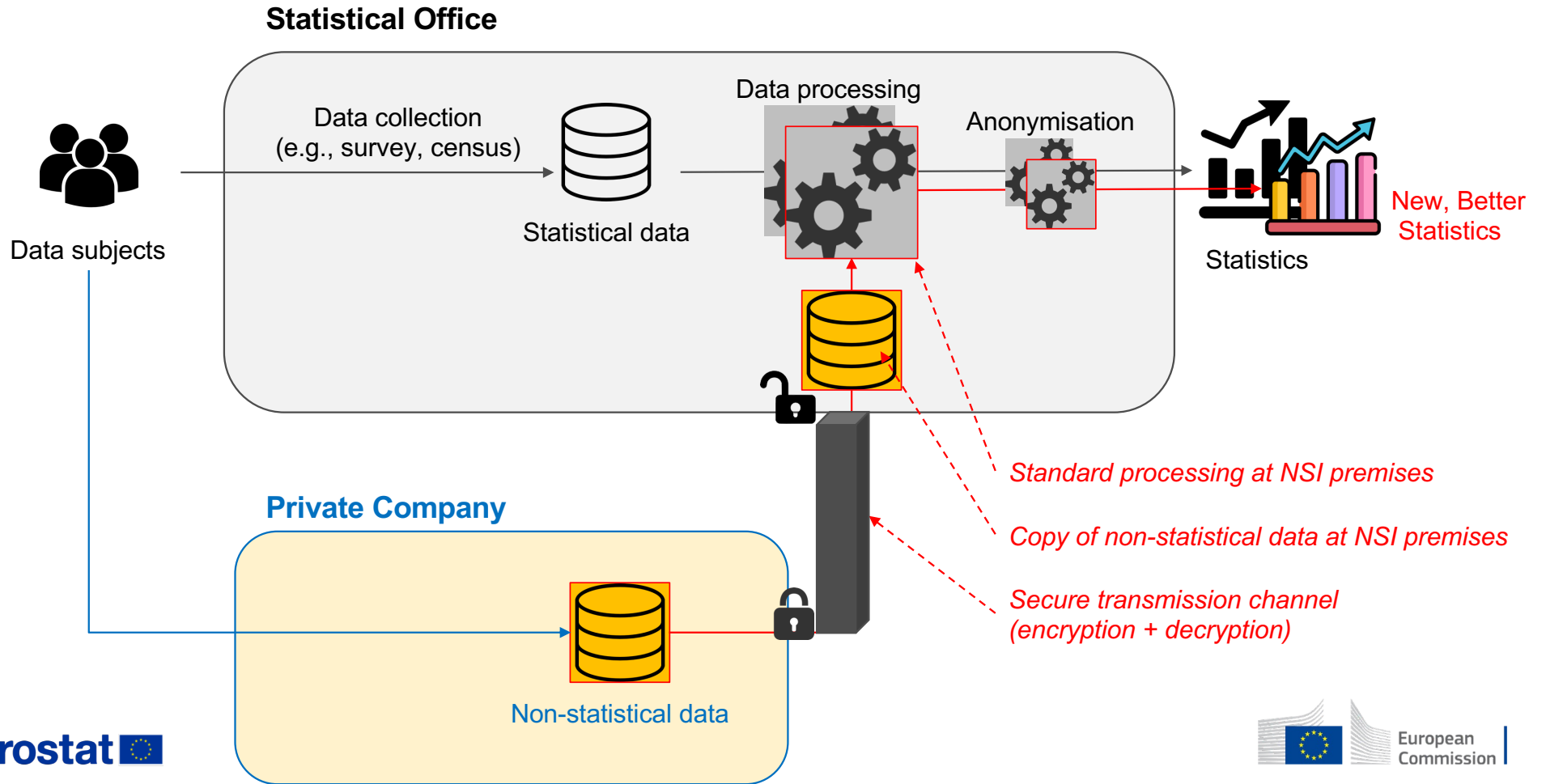
Example use-case: (re)use of Privately Held Data for statistical production



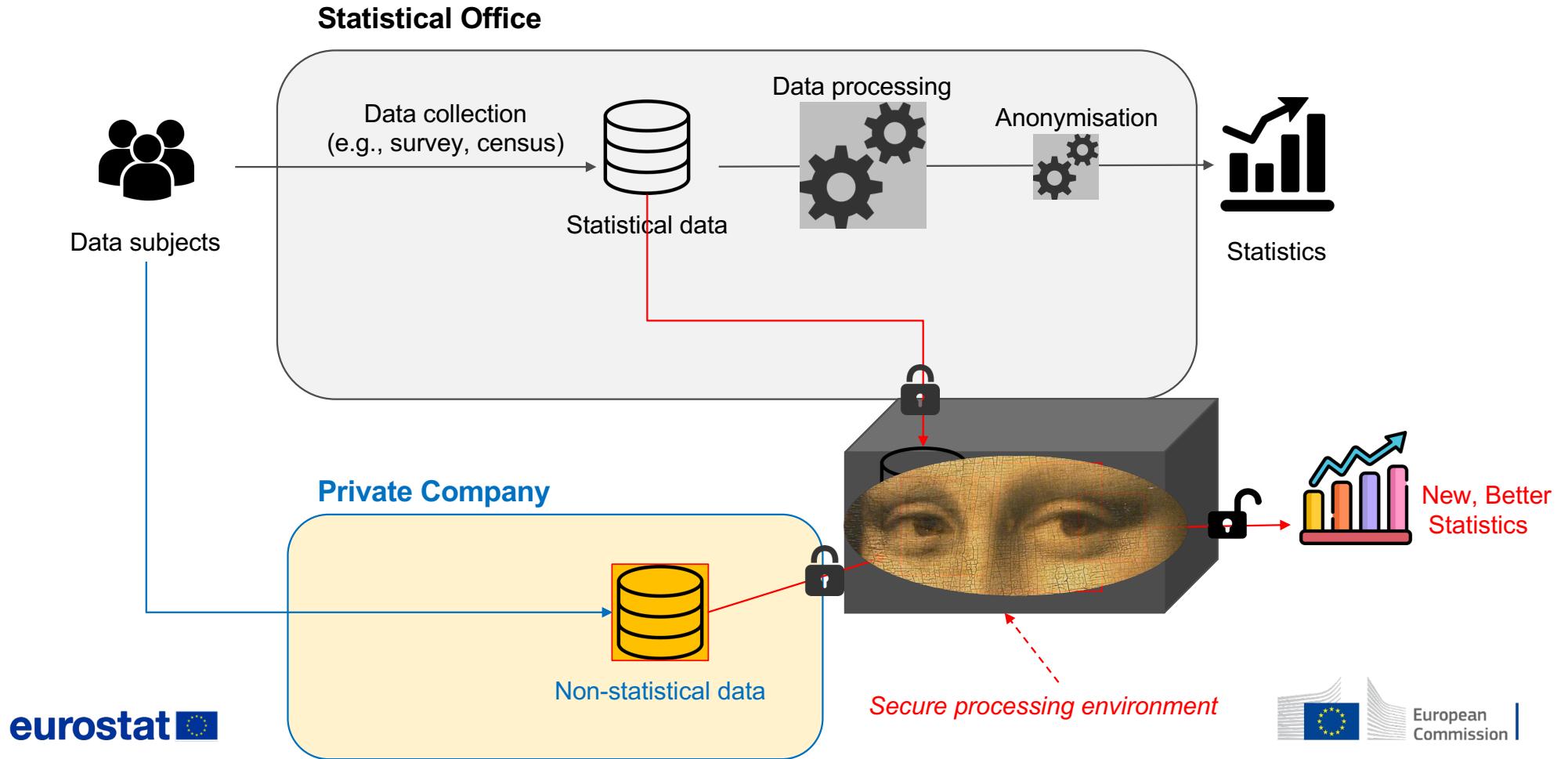
Securing the data sharing



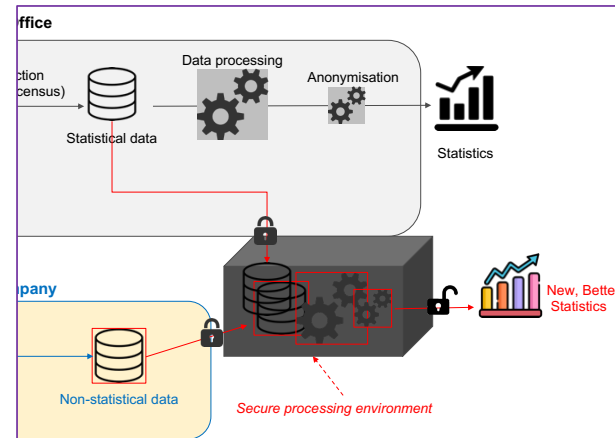
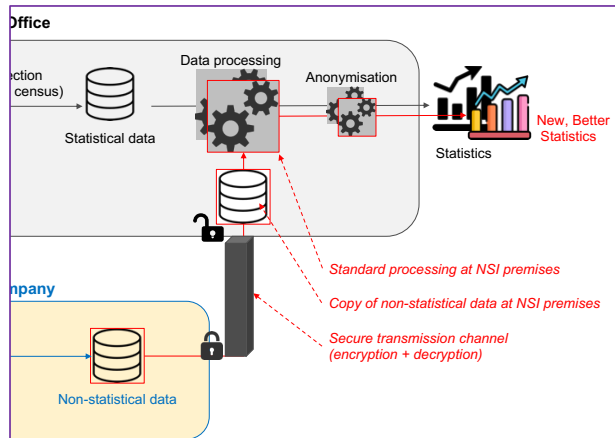
Securing the data sharing

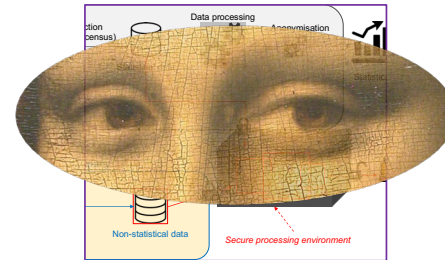
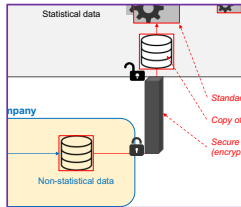
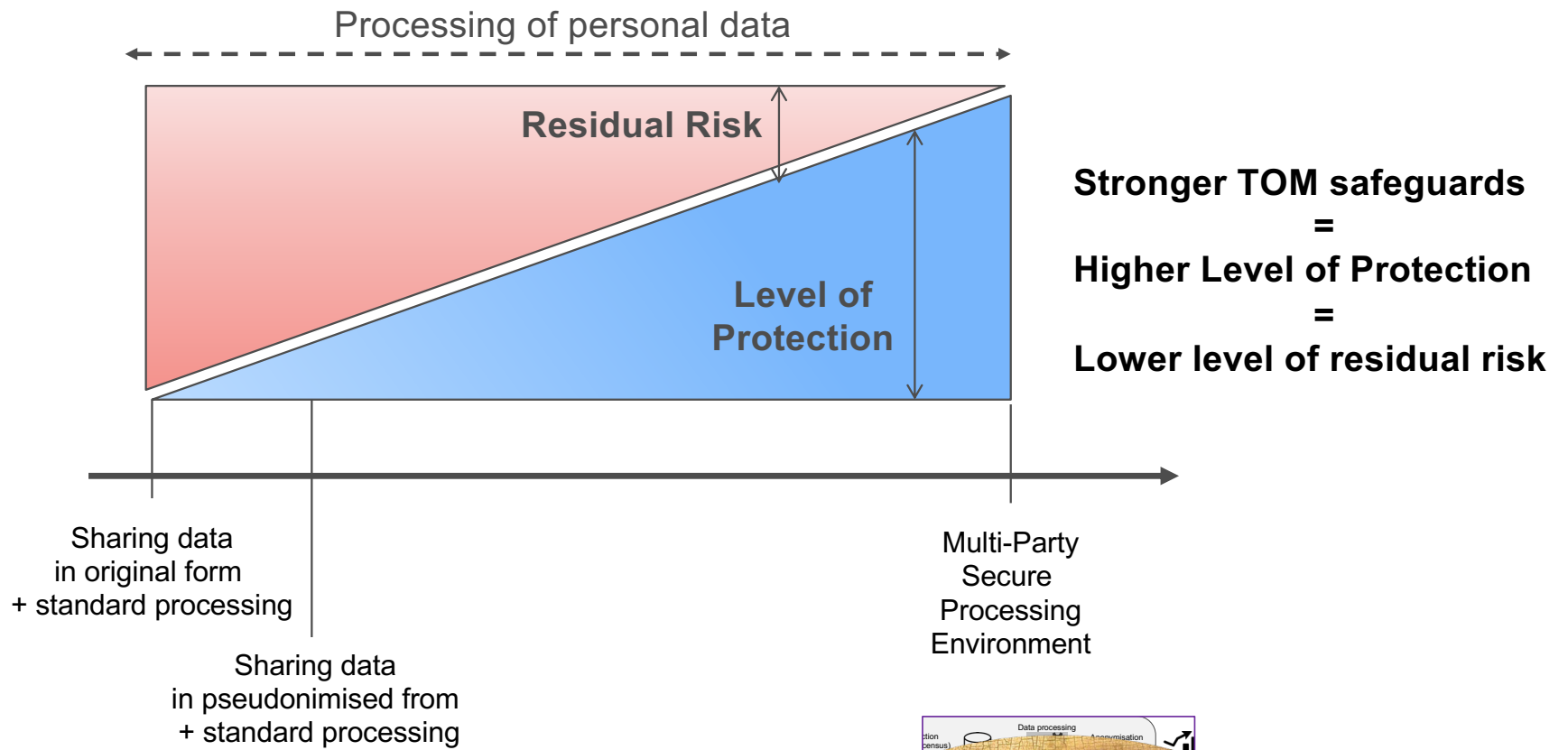


Securing the data processing



Plain data sharing vs Secure processing environment





How do you perform joint processing?

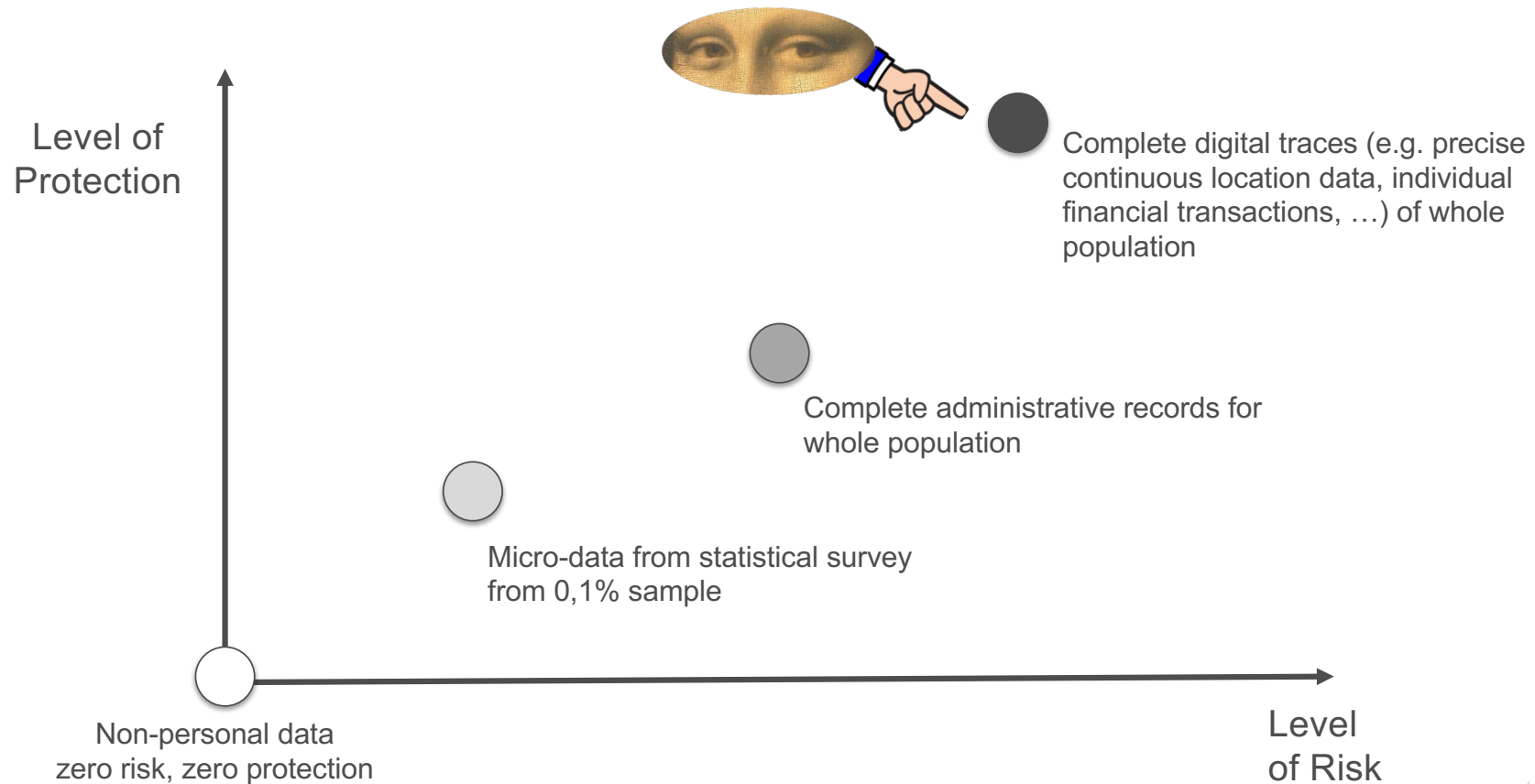
Are you allowed to perform joint processing?

Whether you are allowed to perform joint processing
may depend on
How the joint processing is performed

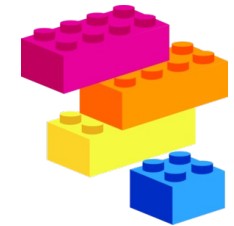
Examples from GDPR:

- “The existence of appropriate safeguards, which may include encryption or pseudonymisation” is part of the compatibility assessment (Art. 6.4)
- Statistical purpose is a compatible secondary purpose subject to appropriate safeguards, i.e., technical and organisational measures (Art. 89)

Proportionality – a key GDPR concept

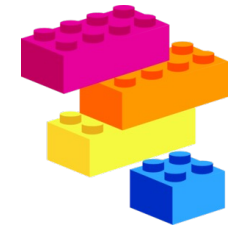


Secure Private Computing (**SPC**)



- Privacy Enhancing Technologies (PET) is an umbrella term comprising two distinct groups of methods/approaches that address distinct (often complementary) problems:
- Input Privacy (aka **Secure Private Computing**, aka Privacy-Preserving Computation)
 - Compute the output without exposing the input (e.g., Computing over Encrypted Data)
 - Multi-Party Computation (MPC) based on secret-sharing, homomorphic encryption, garbled circuits; Trusted Execution Environment (TEE); ...
- Output Privacy (not in the scope of this presentation)
 - Modify the output to avoid disclosing information about the input
 - **Statistical Disclosure Control (SDC)**, Differential Privacy (DP)

Secure Private Computing (SPC)



- Privacy Enhancing Technologies (PET) is an umbrella term comprising two distinct groups of methods/approaches that address distinct (often complementary) problems:



Input Privacy (aka **Secure Private Computing**, aka Privacy-Preserving Computation)

- Compute the output without exposing the input (e.g., Computing over Encrypted Data)
- Multi-Party Computation (MPC) based on secret-sharing, homomorphic encryption, garbled circuits; Trusted Execution Environment (TEE); ...

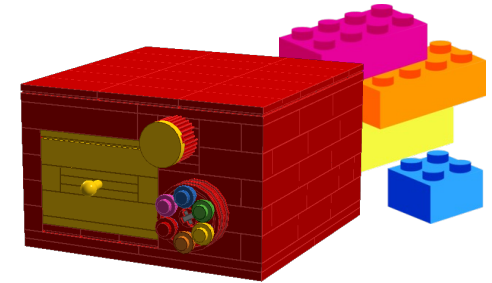
Output Privacy (not in the scope of this presentation)

- Modify the output to avoid disclosing input
- **Statistical Disclosure Control (SDC)**, Differential Privacy (DP)

NOT in the scope
of this project

In the scope
of this project

SPC as a “system” of safeguards



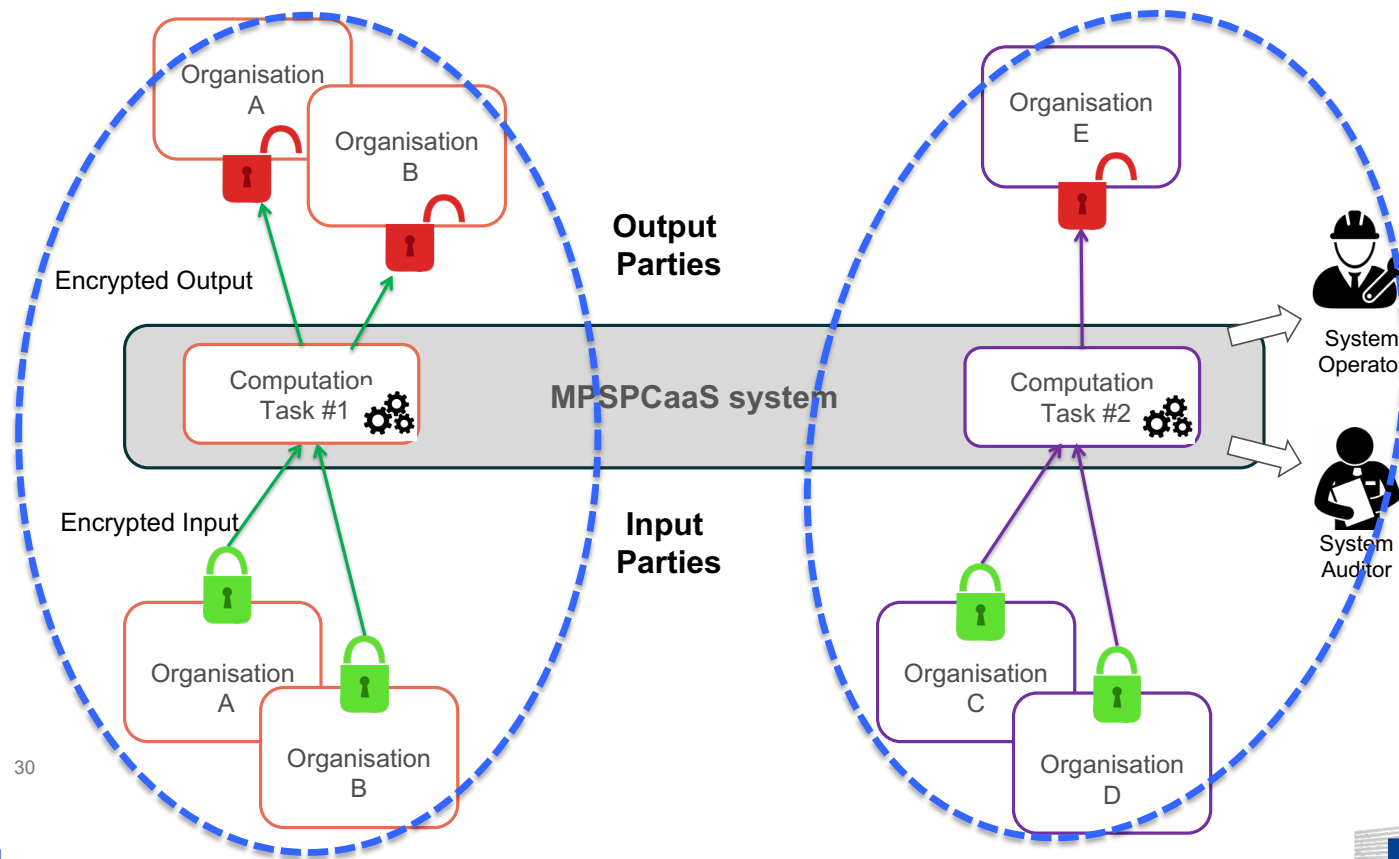
- SPC solution is a **system of safeguards** comprising
 - **Technological** components: MPC, TEE, authentication, encryption,...
 - **Organisational** components: policies, processes, agreements...
 - Fits well with “**Technical and Organisational Measures**” in GDPR, Art. 89

Article 89

Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or **statistical purposes**

1. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to **appropriate safeguards**, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that **technical and organisational measures** are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

Multi-Party Secure Private Computing-as-a-service – MPSPCaaS



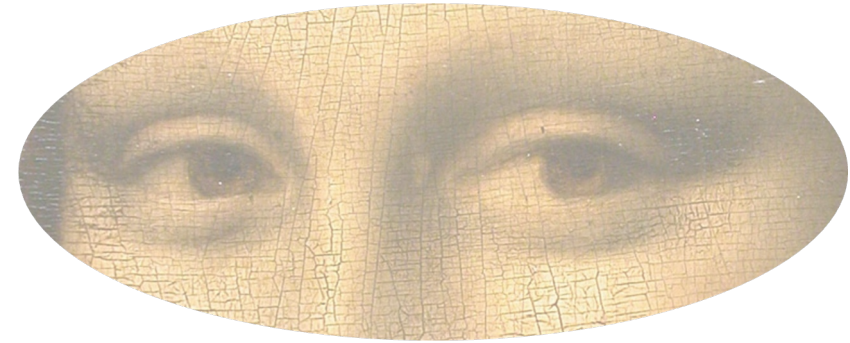
30

MPSPCaaS: from conceptualisation to specification

- 2021 – MPSPCaaS concept first proposed by Eurostat in UNECE HLG-MOS project on Input Privacy Preservation (IPP), 2021-2022
 - Open Technical Consultation organised as part of IPP project; presentations and exchange of ideas with data protection and privacy experts (ENISA workshop, MPC alliance, ...)
- 2023 – Launch of open call for tenders by Eurostat and evaluation of tenders
 - ESTAT/2023/OP/0004 **Specification, feasibility analysis** and **prototype demonstration** of a multi-party secure private computing system for processing confidential sets of micro-data across organisations in support of statistical innovation ([link](#))
- 2024 – Award of contract and launch of JOCONDE project

Reference: *Steps Toward a Shared Infrastructure for Multi-Party Secure Private Computing in Official Statistics*, JOS 03/2024 <https://journals.sagepub.com/doi/10.1177/0282423X241235259>

JOCONDE project



- **Joint On-demand COmputation with No Data Exchange**
 - Started in April 2023, duration 24 months, ending March 2026
 - In collaboration with Cybernetica – Estonian company specialised in security and privacy technologies (<https://cyber.ee>)
- **Goals**
 - **Define MPSPCaaS system specifications** at all levels – technology, organisational, legal – based on extensive analysis of state-of-the-art
 - **Demonstrate** based on **prototype implementation** feasibility, usability, scalability
 - *The results from JOCONDE will enable procurement and deployment of production system in follow-up projects 2026+*

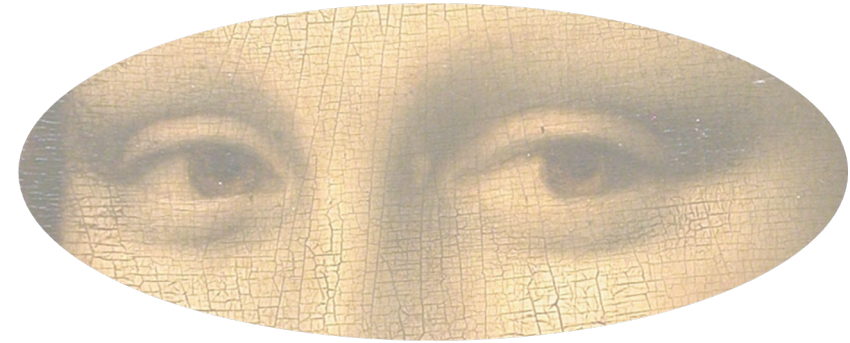
6 Tasks for JOCONDE

- Task 1 – Usage scenarios and system requirements
 - Task 2 – Technology analysis
 - Task 3 – Legal aspects
 - Task 4 – System Specifications and Architecture
 - Task 5 – Demonstrator prototype and functional testing
 - Task 6 – Trust building plan
-
- The diagram illustrates the flow of deliverables and testing phases from the tasks to an external discussion input. It features a list of six tasks on the left. To the right, three red brackets group the tasks into three categories: 1) 'First deliverables D1.1 and D2.1 Now available' (covering Task 1 and Task 2), 2) 'First deliverables D3.1 and D4.1 planned Q1/2025' (covering Task 3 and Task 4), and 3) 'Testing based on demonstrator implementation, possibly involving volunteering NSIs as beta-testers, in Q3/Q4 2025' (covering Task 5 and Task 6). Red lines connect these categories to a red oval at the top right containing the text 'Input for discussion with external experts'.

GDPR principles as system design requirements

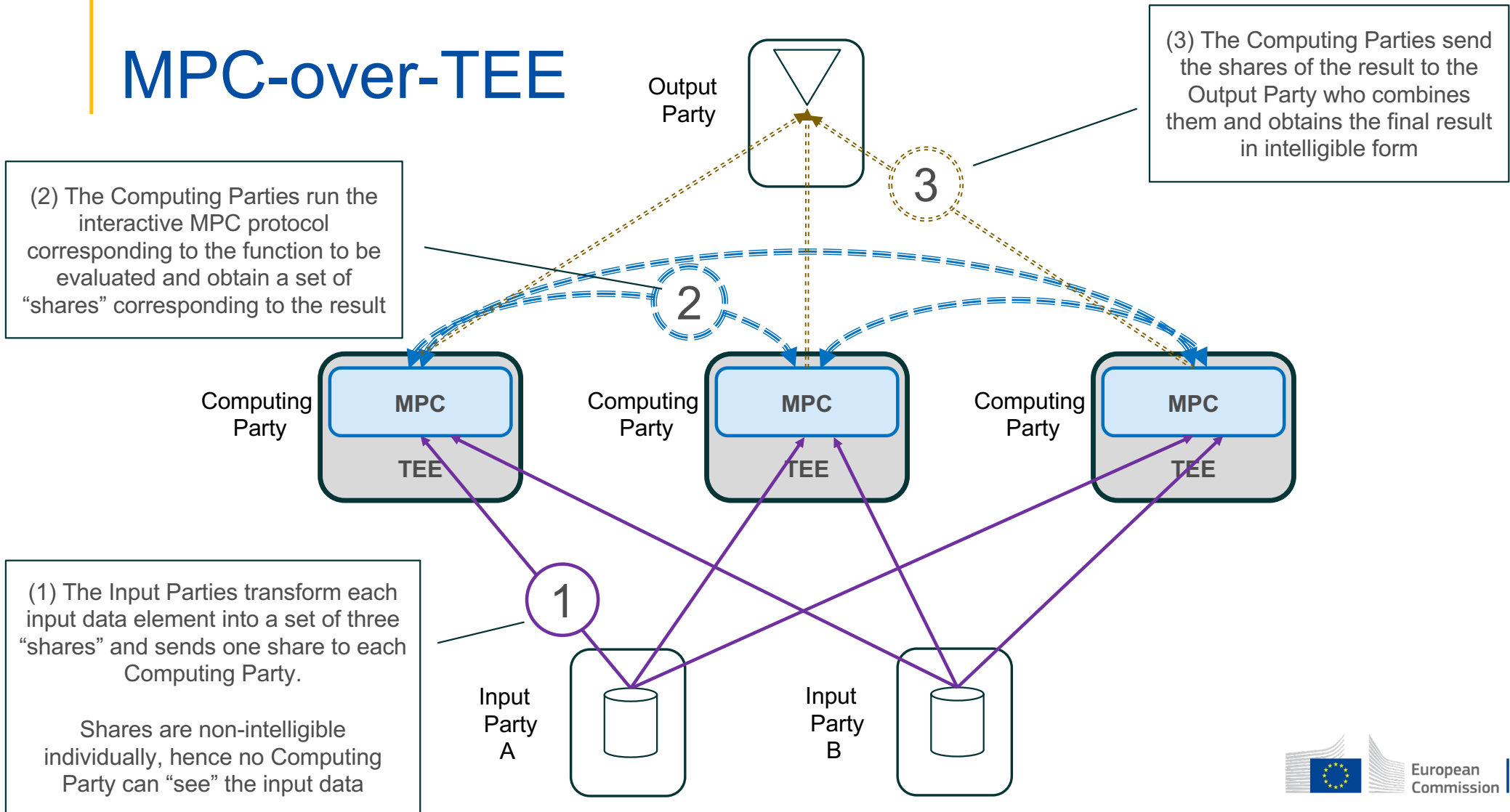
GDPR principle	system feature
Lawfulness, Fairness and Transparency	Each Computation Task executed on the system qualifies as processing of personal data (if the input data represent personal data). The Terms of Use foresee that users must have an appropriate legal basis for each Computation Tasks. System specifications are publicly available.
Purpose limitation	The system adopts technological measures to allow only Computation Tasks that have been explicitly approved by the relevant actors (data controllers) to be executed. The Computation Task specifications include analysis code expressed in a formal language. Technological measures prevent the execution of other analys tasks.
Data minimisation	The system does not disclose anything more than the final computation result (output data minimisation). Furthermore, by their nature MPC protocols disincentivise the processing of data that are not strictly necessary to compute the desired result (input data minimisation)
Accuracy	N.A.
Storage limitation	Upon termination, the system shall securely erase all information exchanged with the nodes in the context of the Computation Task (stateless system) except for logs.
Integrity and Confidentiality	The system incorporates state-of-the-art security technologies to ensure integrity and confidentiality of input and intermediate data
Accountability	The system supports secure logging function to allow independent auditability

Technological approach



- Full overlay MPC over TEE
- Architecture based on 3 logical planes: M-plane, C-plane and D-plane
 - Inspired by telecom and computer network architectures
- D-plane supporting multiple MPC engines, open-source and proprietary
 - Configurable at Computation Task establishment
 - Evolvability – no vendor lock-in – coverage of design space
- Standard programming language with open-source compiler
 - To abstract cryptographic complexity from users

MPC-over-TEE



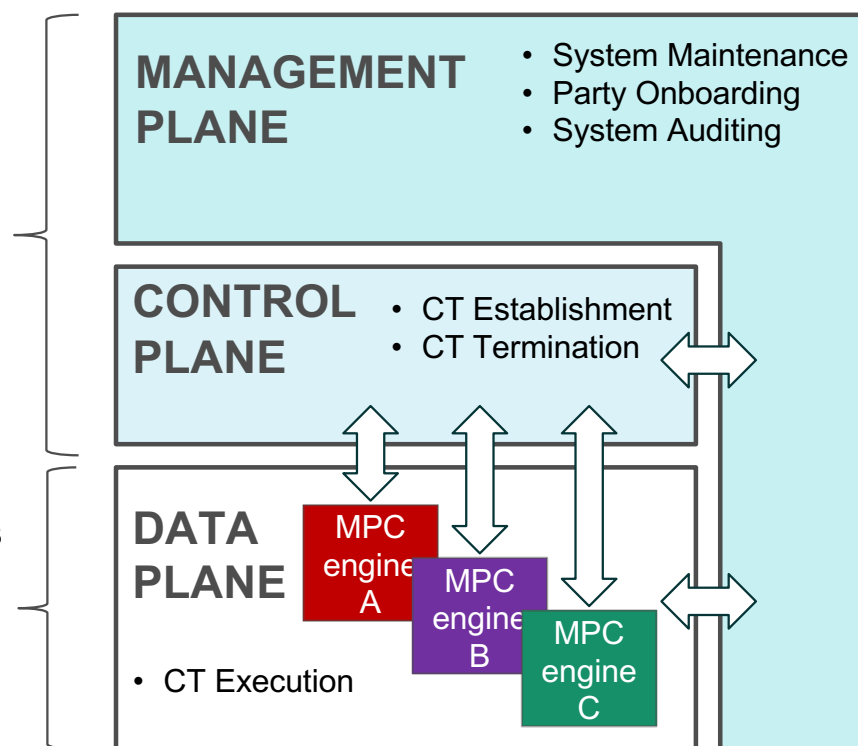
M-plane, C-plane and D-plane

M-plane and C-plane

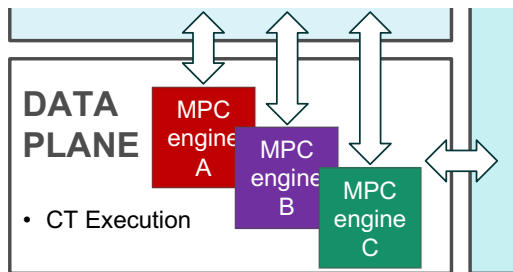
- Developed by JOCONDE
- Fully open-source

D-plane

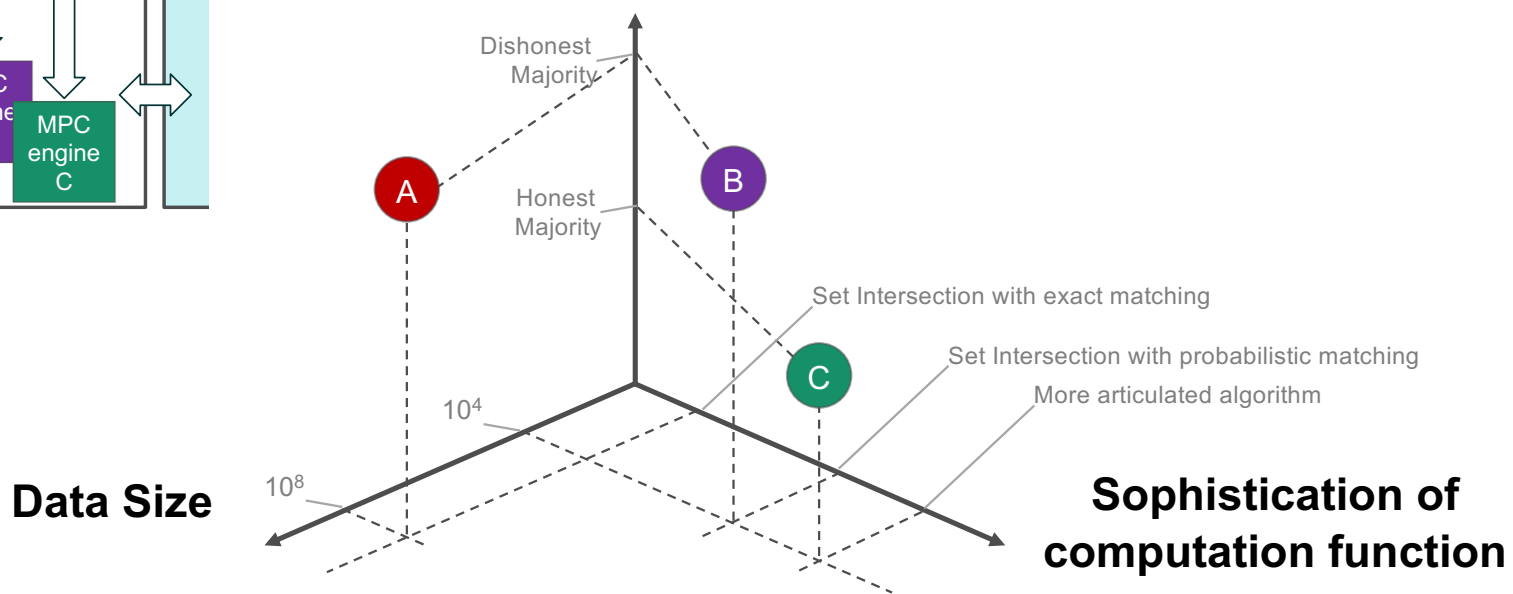
- Reusing existing components
- Supporting multiple TEE platforms
- Supporting multiple MPC engines, open-source and proprietary (selectable on per-CT basis)



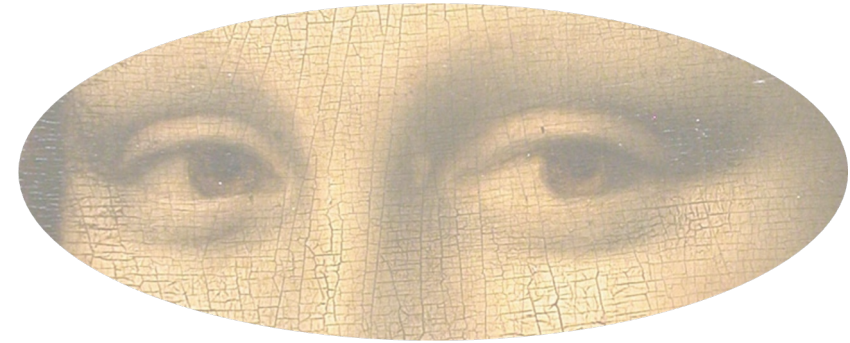
Design space for MPC protocols



Security Guarantees (power of attacker)



Technological approach/2



- Secure deletion of all intermediate data (secret shares, keys,...) except audit logs upon Computation Task (CT) termination
 - Legal implications: liabilities limited to CT execution time
- No Single Point of Trust
 - Otherwise we would be building “just” a very complicated Trusted Third Party
- Not a mission-critical system
 - Availability not a primary design requirement

Demonstrator Prototype \neq Production System

- The system prototype developed in JOCONDE serves multiple purposes
 - Provide a (first version of) **C-plane and M-plane open-source code** to be reused for the future production system (with further extension and consolidation)
 - Proof of concept: demonstrate its technical feasibility and usability as a production system (show it's ready to move from lab to fab)
 - Testing – see if everything works as expected, find problems and fix them
 - Tasting – let some prospective users (beta testers) give it a try and see how they like it

Task 3 – Legal aspects

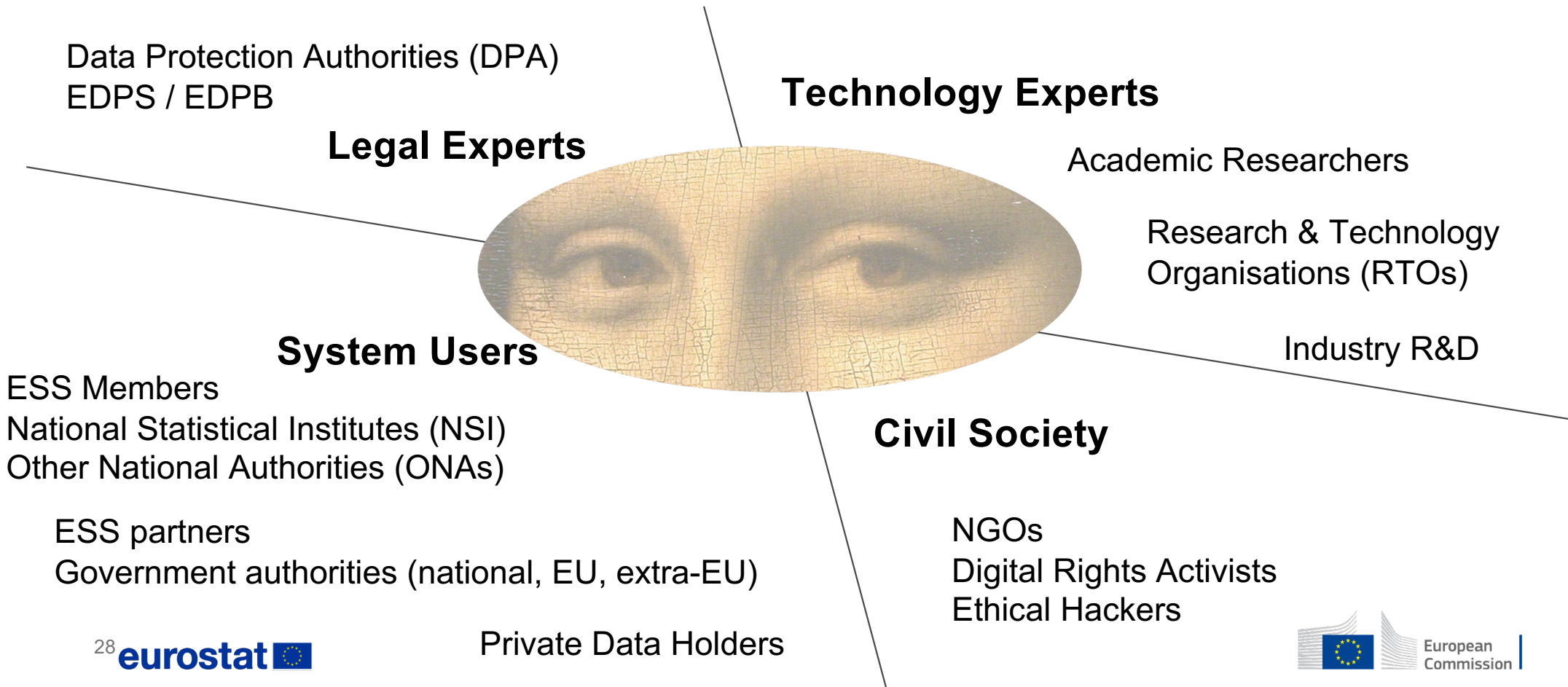


- Task 3 shall perform a **legal analysis** to identify applicable legal requirements and identify open issues
- Task 3 will also prepare **reference legalware** (for CT-independent components) and provide **guidelines** (for CT-specific components)
 - **Reference models of agreements and contracts** between the parties (clarify liabilities, controller / processor roles, etc.)
 - Model of DPIA elements
- **The ultimate goal of Task 3 is to minimise as much as possible the legal burden for prospective users.**

Task 6 –Trust building plan

- Building a Trustworthy System is necessary, not sufficient for Building Trust.
- More is needed to ensure public trust and public acceptance
- How to convince key stakeholders and the general public of the genuinity and strength of the system?
 - Openness and transparency → how in practice?
 - Red team? → how in practice?

Stakeholders



Outlook



- Work in progress towards providing the ESS with a shared platform for on-demand multi-party computation on confidential data, offering alternative to traditional data sharing mechanisms
 - JOCONDE project <https://cros.ec.europa.eu/joconde>
 - Testing activities in late 2025 may possibly involve volunteering NSIs
 - JOCONDE results will enable procurement and deployment of production system in follow-up projects
- For further activities by Eurostat related to Privacy-Enhancing Technologies for Official Statistics refer to <https://cros.ec.europa.eu/PET4OS>

Thank you



© European Union 2024

Unless otherwise noted the reuse of this presentation is authorised under the [CC BY 4.0](https://creativecommons.org/licenses/by/4.0/) license. For any use or reproduction of elements that are not owned by the EU, permission may need to be sought directly from the respective right holders.