iMARS Workshop

WP3 & WP14 – Ethical, Legal and Societal Aspects

Abdullah Elbi, KU Leuven

Els Kindt, KU Leuven

Marek Tiits, Institute of Baltic Studies

Elin Palm, Linköping University

iMARS
image manipulation attack
resolving solutions

30 March 2023
Abdullah Elbi

Overview of WP3 & 14

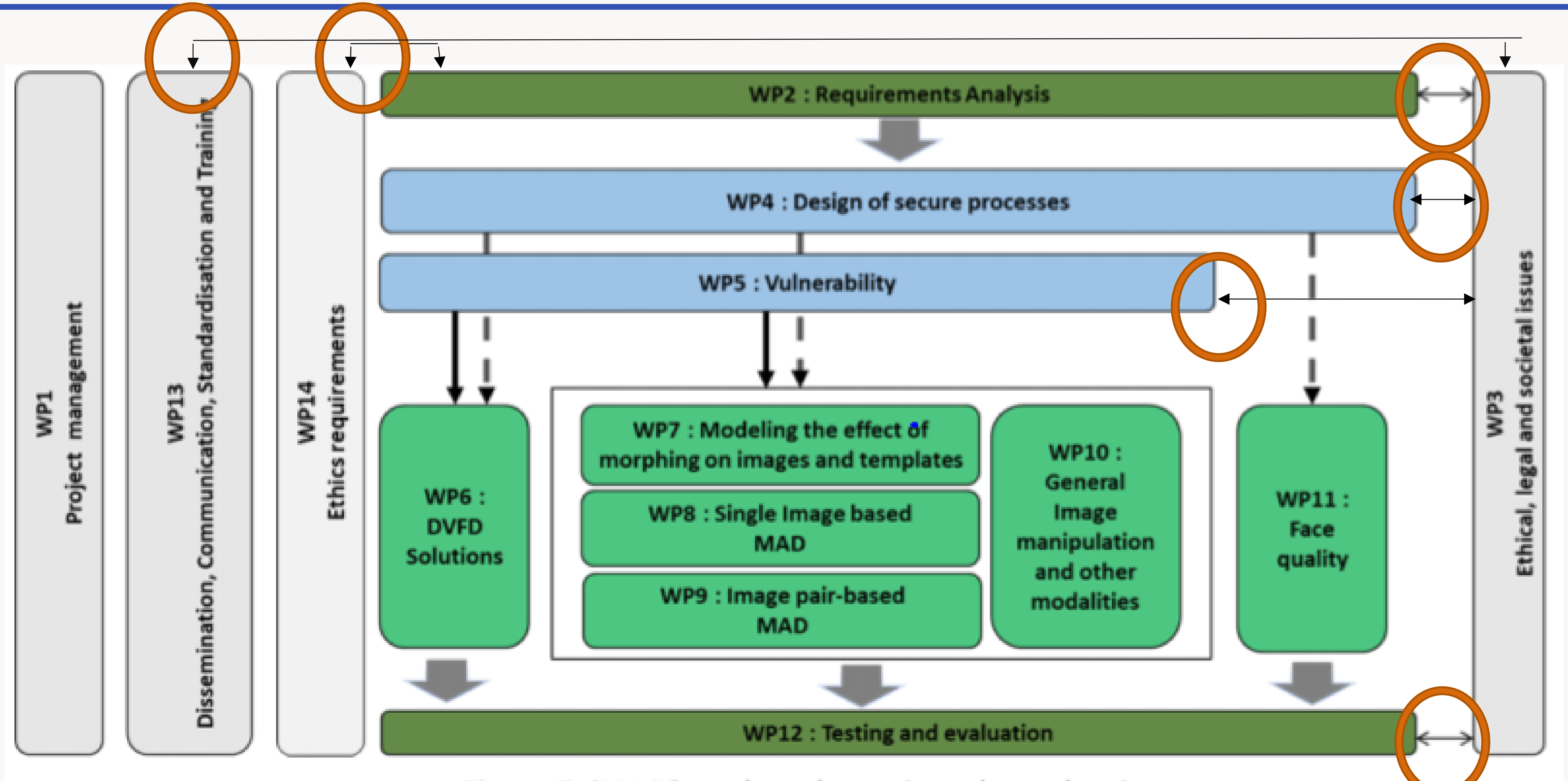

WP1
Project management
WP13
Dissemination, Communication, Standardisation and Training
WP14
Ethics requirements
WP2 : Requirements Analysis
WP4 : Design of secure processes
WP5 : Vulnerability
WP6 : DVFD Solutions
WP7 : Modeling the effect of morphing on images and templates
WP8 : Single Image based MAD
WP9 : Image pair-based MAD
WP10 : General Image manipulation and other modalities
WP11 : Face quality
WP12 : Testing and evaluation
WP3
Ethical, legal and societal issues

Figure 7: iMARS work packages interdependencies

The iMARS project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883356

WP 3 & 14 Objectives

1. Ensure that the iMARS developments are in line with and meet EU legal, ethical, privacy and data protection requirements and used in accordance with societal expectations.
2. Analyse iMARS tools for interoperability of EU large scale systems.
3. Develop guidelines and best practices for detection of manipulation attacks including border control context.
4. Ensure compliance with the relevant ‘ethics requirements’
5. Analyse the potential ethical implications of iMARS technologies by independent Ethics Advisors

The iMARS project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 883356

WP 3 & 14 Deliverables

WP 3 Deliverables

- **D3.1** Legal, ethical and societal requirements (KUL, M13) ✓
- **D3.2** Societal acceptability report (IBS, M18) ✓
- **D3.3** Guidelines and Best Practices (KUL, M36)
- **D3.4** Technology assessment: ethical, legal and societal aspects(KUL, M48)

WP 14 Deliverables (specific)

- **D14.5** First Ethical Assessment (M13) ✓
- **D14.6** Second Ethical Assessment (M36)

The iMARS project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883356

D3.1- Legal, ethical and societal requirements

→ Wide range of legal instruments**: International**, **Supranational**, **National** Legal instruments should be considered for each specific case.

1. Research/Development *Phase:*

- *GDPR and specific MS law on biometric data and research [see Art 9(4) GDPR Art 89 GDPR]*

2. Deployment/Operational *Phase:*

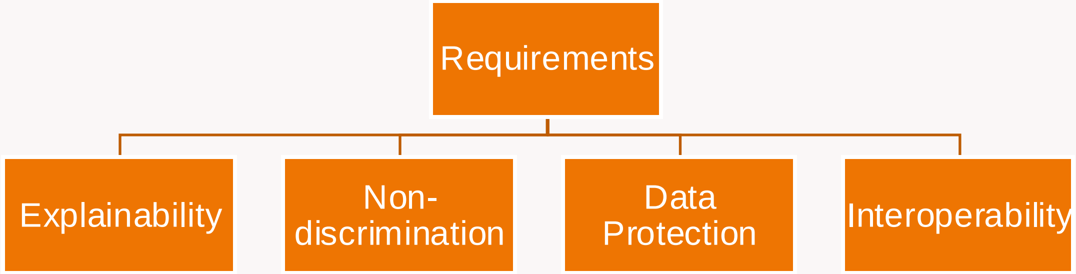
- “Smart Borders” EES Regulation and Schengen Border Code,
- Interoperability Regulation 2019/817 and 2019/818,
- GDPR, EUGDPR and Law Enforcement Directive 2016/680
- AI Act (Proposal)

→ **Demographic Representation** and **Gender Balance** should be prioritized during and after development phase of iMARS tools.

ID issuance

Border control

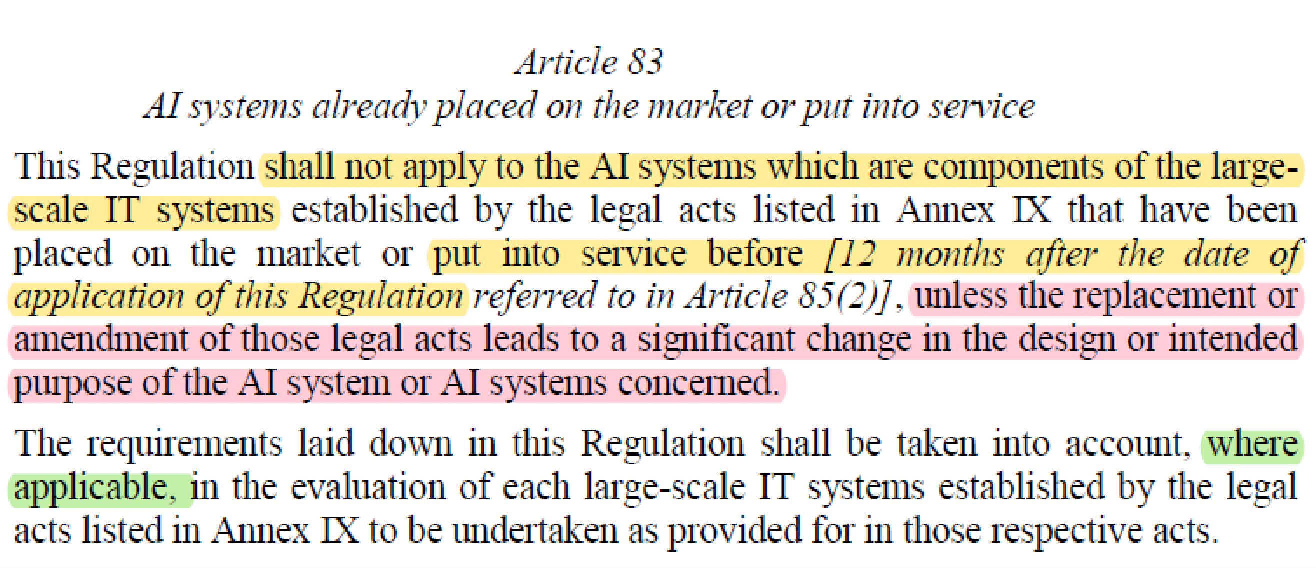
Forensic



AI Act (Proposal) & iMARS Tools 1/2

→ Exclusion of AI components of Large Scale IT systems from the scope of AI Act : SIS, VIS, Eurodac, EES, ETIAS.

→ See also **Annex 3** of the Proposed AI Act



Article 83

AI systems already placed on the market or put into service

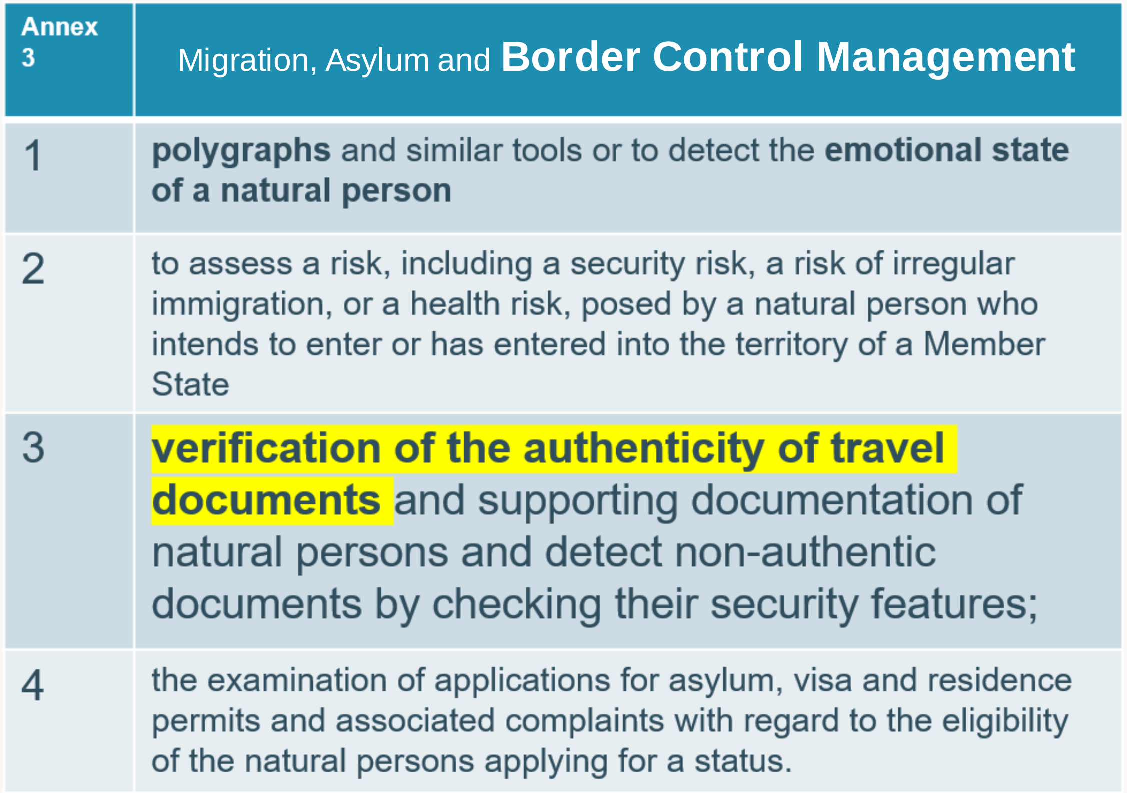
This Regulation shall not apply to the AI systems which are components of the large-scale IT systems established by the legal acts listed in Annex IX that have been placed on the market or put into service before *[12 months after the date of application of this Regulation referred to in Article 85(2)]*, unless the replacement or amendment of those legal acts leads to a significant change in the design or intended purpose of the AI system or AI systems concerned.

The requirements laid down in this Regulation shall be taken into account, where applicable, in the evaluation of each large-scale IT systems established by the legal acts listed in Annex IX to be undertaken as provided for in those respective acts.

? Automated identity verification tools, and document authentication?

The iMARS project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 883356

AI Act (Proposal) & iMARS Tools 2/2



Annex 3	Migration, Asylum and **Border Control Management**
1	**polygraphs** and similar tools or to detect the **emotional state of a natural person**
2	to assess a risk, including a security risk, a risk of irregular immigration, or a health risk, posed by a natural person who intends to enter or has entered into the territory of a Member State
3	**verification of the authenticity of travel documents** and supporting documentation of natural persons and detect non-authentic documents by checking their security features;
4	the examination of applications for asylum, visa and residence permits and associated complaints with regard to the eligibility of the natural persons applying for a status.

→ **Requirements** for High risk AI systems in the context of Migration, Asylum and Border Control Management

- Use **high-quality** training, validation and testing data (relevant, representative etc.)
- Ensure appropriate degree of **transparency** and provide users with information (on how to use the system)
- Establish and implement **Risk Management** processes
- Ensure **Human oversight**
- Ensure **robustness, accuracy** and **cybersecurity**

→The verification of travel documents and supporting documents.[**Removed** from the Annex 3 in the Council's version- late 2022.]

D14.5 First Ethical Analysis

S-MAD and D-MAD may involve different degrees of risk

The use of Synthetic data and/or Personal data

The need for bias mitigation measures and respecting Human dignitiy

Oversight and redress mechanisms

Ethical consent vs data protection consent

First ethical analysis of iMARS technologies conducted by Pr. Elin Palm in M13.

→ **Demographic Representation** and **Gender Balance** should be prioritized during and after development phase of iMARS tools

→ KUL made a change to the consent form to highlight which **ethical principles** iMARS will follow.

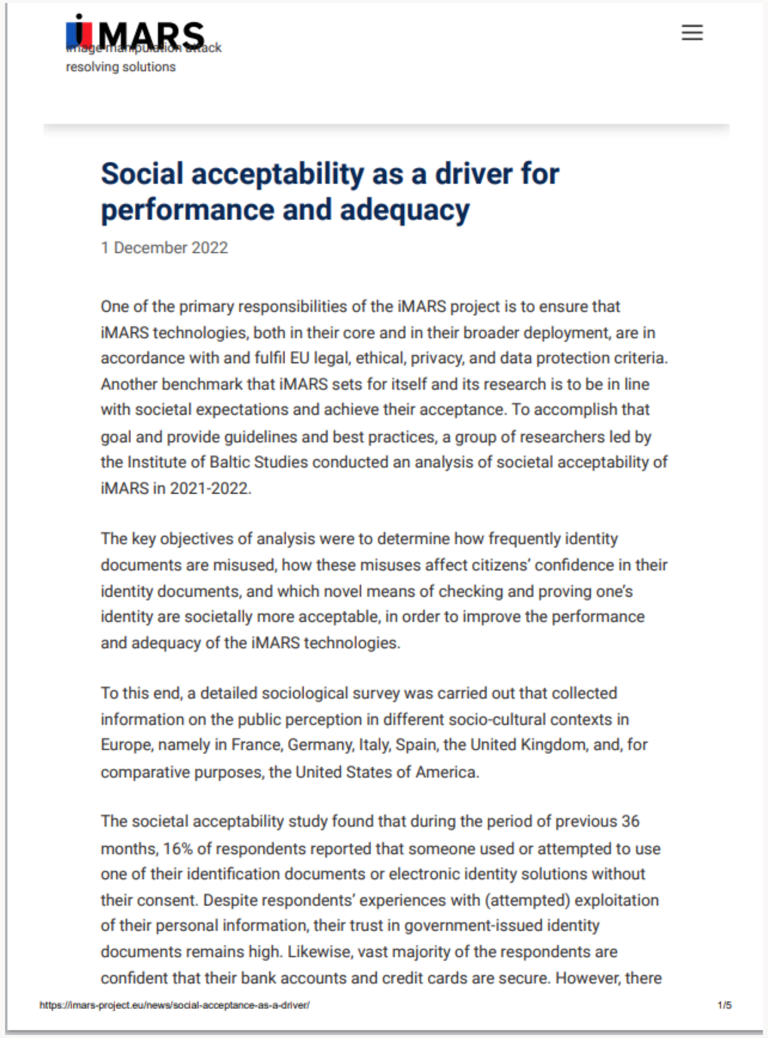
D3.2 Social Acceptability Report

→ A demographically representative sample of 3000 fully completed questionnaires was collected from DE, ES, FR, IT, UK, US in March-April 2022

- 80%+ of respondents believe, nonetheless, that the government issued identity documents are secure

- In sum**, sufficient public support to the technologies that will have been developed in iMARS**, but the purpose and intended use of any personal information is to be explained carefully to citizens.

→ A blogpost published on the iMARS website, available at: https://imars-project.eu/news/social-acceptance-as-a-driver/



iMARS
image manipulation attack
resolving solutions

Social acceptability as a driver for performance and adequacy

1 December 2022

One of the primary responsibilities of the iMARS project is to ensure that iMARS technologies, both in their core and in their broader deployment, are in accordance with and fulfil EU legal, ethical, privacy, and data protection criteria. Another benchmark that iMARS sets for itself and its research is to be in line with societal expectations and achieve their acceptance. To accomplish that goal and provide guidelines and best practices, a group of researchers led by the Institute of Baltic Studies conducted an analysis of societal acceptability of iMARS in 2021-2022.

The key objectives of analysis were to determine how frequently identity documents are misused, how these misuses affect citizens' confidence in their identity documents, and which novel means of checking and proving one's identity are societally more acceptable, in order to improve the performance and adequacy of the iMARS technologies.

To this end, a detailed sociological survey was carried out that collected information on the public perception in different socio-cultural contexts in Europe, namely in France, Germany, Italy, Spain, the United Kingdom, and, for comparative purposes, the United States of America.

The societal acceptability study found that during the period of previous 36 months, 16% of respondents reported that someone used or attempted to use one of their identification documents or electronic identity solutions without their consent. Despite respondents' experiences with (attempted) exploitation of their personal information, their trust in government-issued identity documents remains high. Likewise, vast majority of the respondents are confident that their bank accounts and credit cards are secure. However, there

https://imars-project.eu/news/social-acceptance-as-a-driver/ 1/5

The iMARS project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883356

Next?

What are the existing best practices for the further development and operational phase of the iMars tools?

→Continue to research and develop the **Best Practices/ Guidelines** for Manipulation Attack Detection(MAD) Solutions which **respect fundamental rights** in particular right to privacy and data protection.(M36)

For example:

- “**four eyes**” principle (in particular for border management and law enforcement use case)
- **Tailored fundamental rights** impact assessment of the particular use case.
- **Training** of the agents (i.e. in particular against the automation bias)

The iMARS project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 883356

Next?

Additionally..

→Research activities under the iMars Project must be carried out **in compliance with GDPR** obligations and ethical principles.

→Conduct a literature review for impact assessments and **develop iMARS-tailored impact assessment.**(M48)

→**Developing 2nd** Ethics Report on iMARS tools by Independent Ethics Advisor (M36)

iMARS WORKSHOP

Feel free to use the public chat area or raise you hand to ask your questions to the speaker.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883356.