Privacy and data governance

The third of the seven requirements of Ethics Guidelines for Trustworthy AI refers to "Privacy and Data Governance".

Besides ensuring **full respect for privacy and data protection**, adequate data governance mechanisms must also be ensured, considering the quality and integrity of the data, and ensuring legitimised access to data.

As discussed in the previous article (see here), data quality is pivotal for the robustness of AI systems. On top of that, it is important to ensure that AI systems **respect privacy, manage data responsibly, and comply with relevant regulations and ethical standards.** Thus, the assessment of this key requirement should focus on several critical aspects:

Compliance with Legal Frameworks

AI systems must comply with existing legal requirements regarding data privacy and protection, such as the General Data Protection Regulation (GDPR), the Data Act, **the** Data Governance Act, and more. Assessment involves verifying that the AI system adheres to these regulations by implementing necessary data protection and privacy measures, obtaining explicit consent from users, and allowing individuals to exercise their rights (e.g., access, rectification, erasure, etc.) concerning their data.

Figure 1: Data Governance Act

For cases that are likely to involve “a high risk” to other people's personal information, a Data Protection Impact Assessment (DPIA) is also required under the GDPR. Accordingly, additional **ethical reviews may be required, depending on the application scenario, to identify and mitigate potential risks to individuals' privacy and rights.** Engaging stakeholders and obtaining their feedback can also be part of this assessment to ensure a broad perspective on potential ethical implications.

Data Minimization and Purpose Limitation

AI systems should collect and process only the data necessary for their specified purpose, and data should not be repurposed without proper justification and user consent. Assessing this aspect involves **reviewing data collection and pre-processing practices, ensuring that only relevant data is collected, and confirming that the purposes for data processing are clearly defined and adhered to.**

Transparency and Data Governance

Transparency in data handling practices is essential. Organizations must provide clear and accessible information about **how data is collected, used, stored, and shared.** Assessing transparency involves evaluating the clarity and comprehensiveness of privacy policies and data governance frameworks. This includes checking whether users are adequately informed about data practices and whether these policies are publicly available and easy to understand and used (e.g., users are able to opt in or out of data sharing).

Security Measures

Robust security measures are crucial to protect data from unauthorized access, breaches, and other threats. **Assessing data security involves examining the technical and organizational measures in place, such as encryption, access controls, regular security audits, and incident response plans (among others).**

The effectiveness of these measures in safeguarding data throughout its lifecycle (collection, processing, storage, and disposal) should be rigorously monitored and evaluated. Such security mechanisms should also flag and inform about privacy issues, while also providing verification that data are unharmed and have not been compromised.

Accountability and Governance Structures

Clear accountability mechanisms and governance structures must be in place to oversee data privacy and protection efforts. **Assessment involves reviewing the roles and responsibilities of those involved in data management, ensuring there are designated personnel (e.g., a Data Protection Officer) or teams responsible (with appropriate access rights) for data governance, and verifying that there are clear procedures for monitoring compliance and addressing data privacy issues, aligned with relevant standards and protocols.**

Data Privacy and Governance in MANOLO

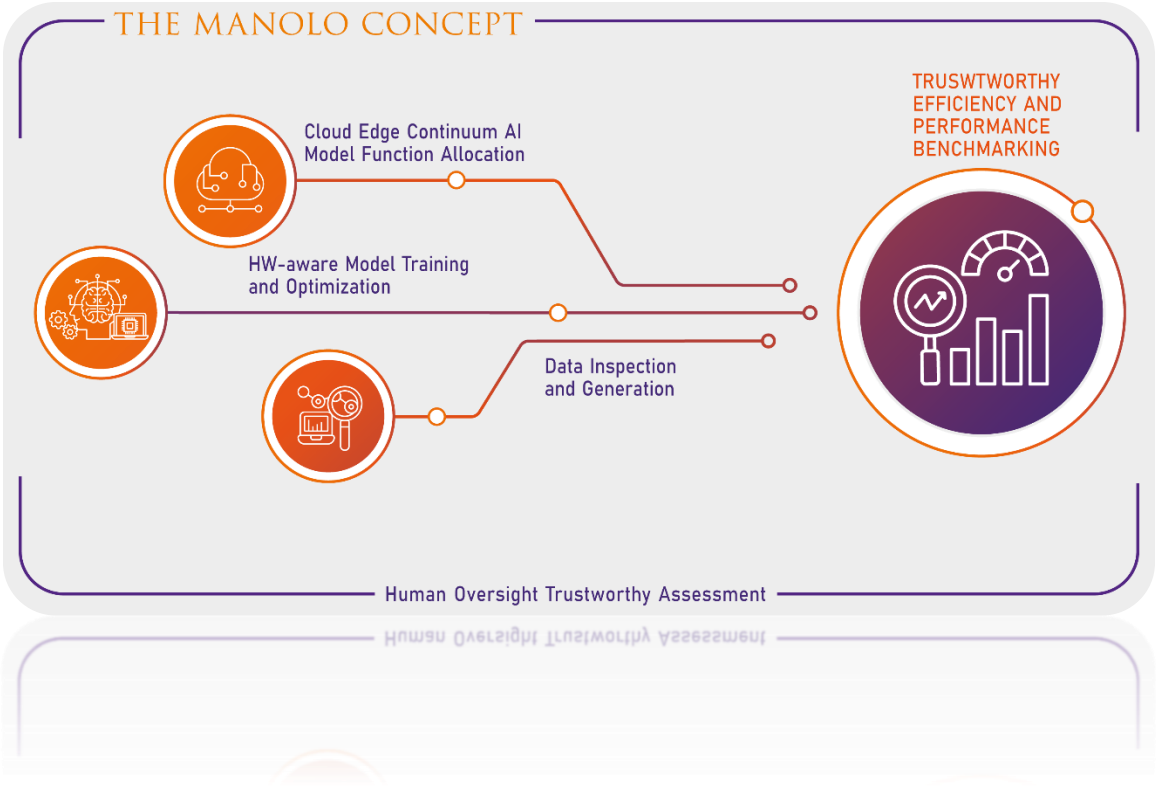

Figure 2:MANOLO concept

Under the guidance of the [National Centre for Scientific Research "Demokritos"](), [MANOLO]() partners will deliver a **Data Management and Provenance Framework** (led by [ARX.NET]()) that will address by design all the critical aspects for Data Privacy and Governance.

Moreover, in cases where data is not available or available data does not suit our objectives on efficiency, distilled high-quality data and meta-data will be synthesised (led by [NUIDUCD-CeADAR]()) using advanced methods such as **data distillation,**

data compression and hashing, feature extraction, and synthesisation, as well as model inversion for synthesisation of data from labels.

Along the way, through detailed Z-Inspection® socio-technical scenarios, MANOLO partners will carefully **examine data privacy and governance concerns within the MANOLO use cases and for the MANOLO components and system.**

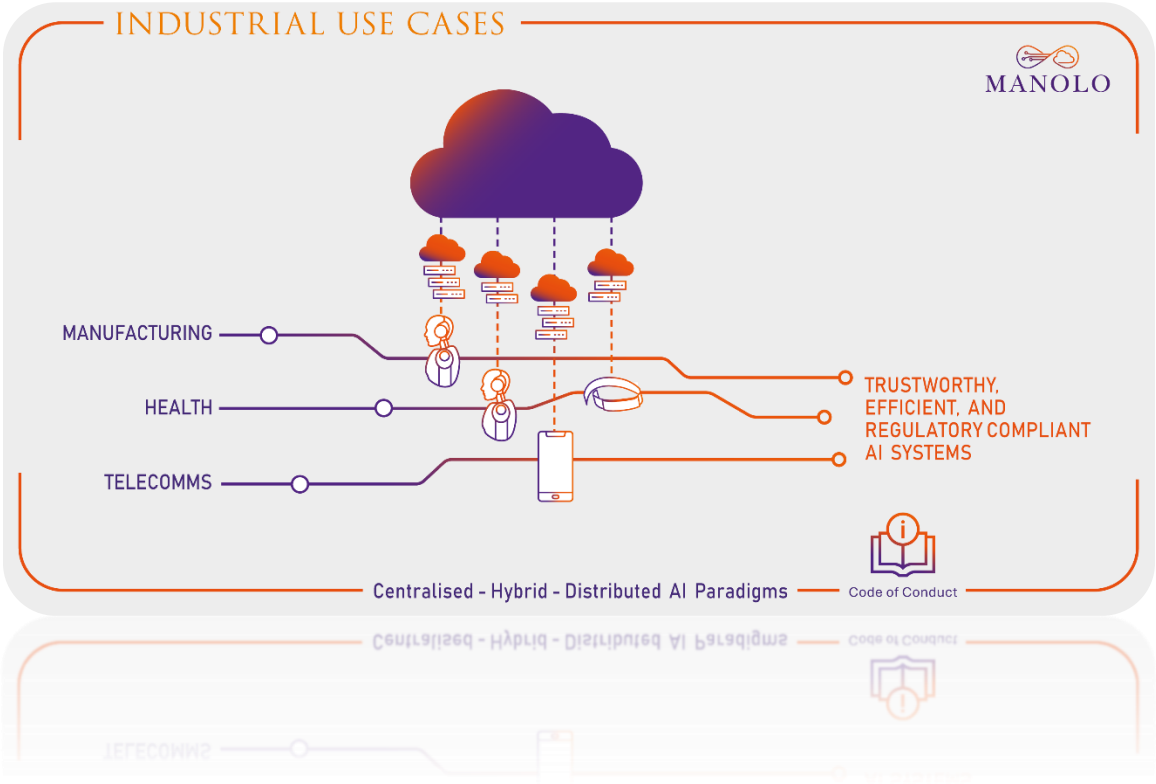

Figure 3: MANOLO Use Cases

Finally, the MANOLO Data Management Plan (led by Q-PLAN International Advisors), sets out the overall methodological principles **pertaining to the management of the data that will be collected, generated, and/or re-used in the framework of MANOLO**, safeguarding sound, and ethical data management along the entire duration of the project.

Wrap Up

Ensuring data privacy and governance in AI systems involves several critical steps. Firstly, **AI systems must comply with legal frameworks (i.e., Data Act, Data Governance Act, GDPR).** This includes implementing data protection measures,

obtaining user consent, and allowing individuals to exercise their rights over their data.

AI systems should also follow data minimization and purpose limitation principles, collecting only necessary data and using it strictly for its intended purpose. Transparency is crucial; organizations must clearly communicate how data is handled and provide options for users to opt in or out of data sharing.

Security measures, including encryption and regular audits, are essential to protect data from breaches. Finally, **clear accountability structures**, including designated data protection officers, must be in place to oversee data governance.

In the MANOLO project, fully address this key requirement through a dedicated Data **Management and Provenance Framework**. MANOLO also uses advanced methods to synthesize high-quality data when necessary. The project's Data Management Plan, managed by Q-PLAN International Advisors, ensures ethical data management throughout its duration.