



# POLICY BRIEF

15 05 2024

14

## DATA GOVERNANCE IN THE AI ACT

ARIANNA ROSSI



| Data governance in the AI Act       |  |
|-------------------------------------|--|
| BACKGROUND AND FIELD OF APPLICATION | <p>Data governance concerns the <b>management of data during its entire lifecycle</b>, from collection to disposal.</p> <p>The European Commission's Guidelines on trustworthy AI<sup>1</sup> drafted by the High-Level Expert Group on Artificial Intelligence have listed data governance, alongside privacy, as one of the fundamental requirements that AI systems should meet to ensure their trustworthiness. Here, data governance concerns the <b>management of the quality and integrity of data, its relevance for the domain</b> where the AI will be deployed, and the <b>protocols for data access</b>. It also concerns the ability to process data while <b>protecting privacy to avoid unlawful and unfair discrimination</b>, especially when AI systems are able to infer personal information such as sexual orientation, age, gender, religious or political views.</p> <p>Clearly echoing this principle, the AI Act provides more specific requirements that are important for the design, training and testing of <b>high-risk AI systems</b> (see Policy brief no. 13) to ensure that they behave as intended and safely, and that they do not enable unlawful discrimination.</p> |
| HIGHLIGHTS                          | <p>Data governance (Article 10) mandates that the <b>datasets used for training, validation and testing are appropriate</b> for the intended use of the AI system.</p> <p>Providers of high-risk AI systems should put in place <b>practices for managing data</b> concerning:</p> <ul style="list-style-type: none"> <li>• The design choices</li> <li>• The processes of data collection and the origin of data; when personal data, the original purpose of collection</li> <li>• Pre-processing operations such as annotation, labelling, cleaning, updating, enrichment and aggregation</li> <li>• Formulation of assumptions, in particular about what the data are supposed to measure and represent</li> <li>• The evaluation of the availability, quantity and suitability of the data sets that are needed</li> <li>• An analysis intended to uncover possible biases that are likely to affect the health and safety of persons, have a negative impact on fundamental rights or lead to unlawful discrimination</li> <li>• The design of measures that prevent, detect and mitigate such biases.</li> </ul>  |

<sup>1</sup> High-Level Expert Group on Artificial Intelligence, 'Ethics Guidelines for Trustworthy AI' (European Commission 2019) <[https://ec.europa.eu/newsroom/dae/document.cfm?doc\\_id=60419](https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419)>.



|                                 |  |
|---------------------------------|--|
|                                 | <p><b>Datasets should be relevant, representative</b>, and, to the best extent possible, <b>free of errors and complete</b>, considering the intended purpose of the AI system. They must have appropriate statistical properties, for example about the people that will be impacted by the system. Biases can be already present in datasets (e.g., when historical data is used) or be generated when the AI system is deployed in real-world settings. This can reproduce or exacerbate existing discrimination.</p> <p>Data sets should also account for the elements that are <b>specific to the specific geographical, contextual, behavioural or functional setting</b> where the high-risk AI system is intended to be used.</p> <p>Whenever <b>personal data are processed</b>, the GDPR principles must be respected, in particular:</p> <ul style="list-style-type: none"> <li>- <b>data protection by design and by default</b>: consider data protection and privacy issues upfront and put in place appropriate technical and organisational measures to protect personal data effectively, for example in terms of security measures that should be adopted to avoid data breaches and leakages.</li> <li>- <b>data minimisation</b>: only collect and process the data that is necessary to achieve a specific purpose</li> </ul> |
| <p><b>IMPACT ON PROJECT</b></p> | <p>The requirement on data governance also <b>impacts other requirements</b> for high-risk AI systems. For example, to <b>achieve transparency</b>, developers need to provide information about the input data and information that can help users to interpret the output, as well as the accuracy of the model (see Article 13). Moreover, the required <b>technical documentation</b> needs to contain information about the training data sets used: about their provenance, scope and main characteristics; how the data was obtained and selected; labelling procedures (e.g. for supervised learning), and data cleaning methodologies (e.g. outliers detection) (see Article 11 and Annex IV). Especially when there is the risk of bias and unlawful discrimination, relevant information about data governance is also useful to determine and maintain the <b>risk management system</b> (Article 9) and to enable <b>human oversight</b> (Article 14) to prevent or minimize harm.</p> <p>The guidelines for EU researchers on “Ethics By Design and Ethics of Use Approaches for Artificial Intelligence”<sup>2</sup> offer additional helpful details on data governance, for instance on how to ensure that fairness and accuracy are accounted for in data collection and preparation and on the</p>                              |

<sup>2</sup> European Commission. Directorate General for Research and Innovation., ‘Ethics By Design and Ethics of Use Approaches for Artificial Intelligence’ (2021) <[https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-by-design-and-ethics-of-use-approaches-for-artificial-intelligence\\_he\\_en.pdf](https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-by-design-and-ethics-of-use-approaches-for-artificial-intelligence_he_en.pdf)> accessed 18 April 2024.



safe deployment of AI. Further, determining the means and policies for the use of data along the AI development lifecycle is also part of the more **general research ethics duty of appropriate data management**, which contributes to research integrity. Many scientific publication venues also encourage authors to submit their digital artefacts, such as datasets, for transparency and reproducibility purposes.

Lastly, this requirement is closely related to the **availability of data enabled by other regulations**, such as the Data Governance Act and the domain-specific data spaces, for instance the European Health Data Space.<sup>3</sup> Data spaces intend to establish trustworthy settings for secure access to and processing of a wide range of data. They set up mechanisms and infrastructures for facilitating **safe-by-design and privacy-friendly data sharing** with the goal of supporting research and innovation.

<sup>3</sup> [https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space\\_en](https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en)