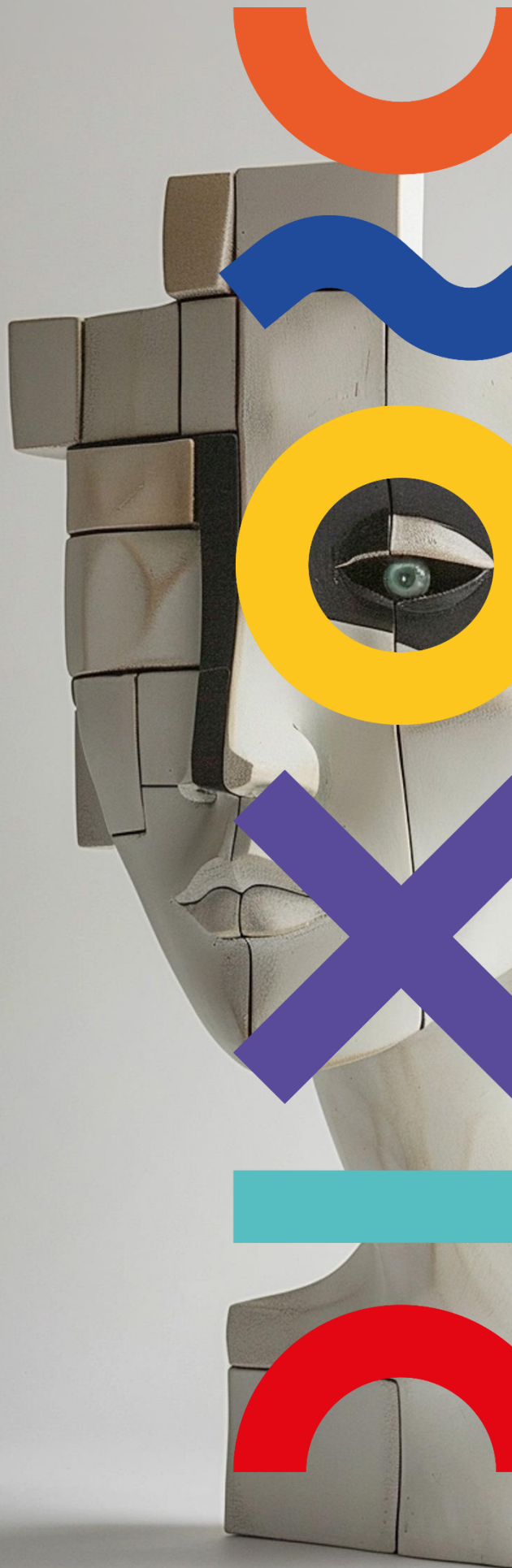# D1.2

Data Management Plan

D1.2 Data Management Plan

Dissemination Level: PU - Public
Lead Partner: ASM
Due date: 30.09.2024
Actual submission date: 30.09.2024

PUBLISHED IN THE FRAMEWORK OF
ENCODE - Unveiling emotional dimensions of politics to foster European democracy consumers

AUTHORS
Małgorzata Walczak – Gomuła, ASM
Joanna Syrda, ASM
Łukasz Wilczyński, ASM

REVISION AND HISTORY CHART

VERSION	DATE	EDITORS		COMMENT
0.1	03.07.2024	Małgorzata Walczak – Gomuła, Joanna Syrda, Łukasz Wilczyński	ASM	Draft
0.2	10.09.2024	Agnieszka Kowalska	ASM	Internal review
0.3	19.09.2024	Łukasz Wilczyński	ASM	Second draft sent for review
0.4	26.09.2024	Seyma Celem	RIE	Review
0.5	27.09.2024	Łukasz Wilczyński	ASM	Update according to comments
1.0	30.09.2024	Aleksandra Oleksik	ASM	Submission to Participant Portal

DISCLAIMER
The information in this document is subject to change without notice. Company or product names mentioned in this document may be trademarks or registered trademarks of their respective companies.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Data Management Plan (DMP) for the ENCODE project is designed to provide a structured approach to managing data throughout its entire lifecycle, ensuring the proper handling of data from collection to destruction. This plan outlines the procedures for collecting, storing, processing, and sharing data while ensuring compliance with both EU and national regulations, particularly GDPR. The DMP is a key part of the project's aim to promote transparency, accountability, and accessibility in research data, in line with the FAIR (Findable, Accessible, Interoperable, and Reusable) principles.

ENCODE will collect a wide variety of data, including social media sentiment analysis, surveys, interviews, and biometric data. The project will focus on understanding the emotional dimensions of political engagement and democratic processes, utilizing advanced machine learning techniques and Natural Language Processing (NLP) to analyse large datasets. Data collection will involve multiple stakeholders, including citizens, policymakers, and marginalized groups, through both qualitative and quantitative research methods.

Data accessibility is a core component of the DMP. All collected data will be made publicly available through the ENCODE project website, scientific publications, and open repositories. The project will ensure that data is properly stored, anonymized, and secured, with access limited to authorized personnel. After the project ends, procedures for data retention and destruction will be followed, ensuring that only necessary data is retained while outdated information is securely deleted.

The ENCODE DMP also includes provisions for updating the plan as needed throughout the project's lifecycle, ensuring that it remains responsive to new data, changes in partner composition, and evolving data management practices. This plan supports the broader goals of the ENCODE project by providing a robust framework for managing and sharing research data, contributing to the creation of new narratives that foster democratic resilience and engagement.

1 INTRODUCTION

1.1 THE ENCODE PROJECT

The ENCODE project, titled "Unveiling Emotional Dimensions of Politics to Foster European Democracy," aims to explore and decode the role of emotions in political discourse and their impact on democratic processes. Recognizing that emotional appeals have significantly influenced political movements and voter behaviour, ENCODE seeks to understand the interplay between emotions, values, and identities. The project's primary goal is to create new positive narratives that can foster trust and engagement in European democratic processes, thereby counteracting the negative emotions that often dominate political discussions. Through innovative methodologies, including social media sentiment analysis, biometric research, and surveys, ENCODE aims to provide policymakers with tools and strategies to better incorporate the emotional needs of citizens into governance, ultimately enhancing democratic resilience and fostering a more inclusive political environment.

1.2 OBJECTIVES OF DELIVERABLE

The **Data Management Plan (DMP)** is a crucial aspect of effective data handling in any research project under **Horizon Europe**, ensuring the smooth integration and reuse of data and knowledge. In the **ENCODE project**, a dedicated task (T1.4) has been established to oversee data management. The DMP will detail the entire data lifecycle for the information collected, processed, and generated in **ENCODE**, particularly focusing on the handling of research data during and after the project, types of data collected, processed, or generated, methodologies and standards applied, open access data, and how the data will be maintained after the project concludes.

As part of the **Open Research Data Pilot (ORDP)**, this deliverable requires **ENCODE project** not only to develop a DMP as a formal deliverable but also to provide open, free-of-charge access to digital research data generated during the project. The DMP will be updated as needed, particularly if significant changes arise, such as the collection of new data not initially planned, changes in partner policies, consortium composition adjustments (e.g., new partners joining or existing partners leaving the project), or other external factors. Monitoring of the data management plan will occur every six months to ensure ongoing compliance and relevancy[1].

1.3 STRUCTURE OF THE DOCUMENT

The deliverable is structured in the following sections:
- Chapter 1 – Introduction to the deliverable.
- Chapter 2 – Procedures for Data Management in ENCODE project.

---

[1] H2020 Programme Guidelines on FAIR Data Management in Horizon 2020, Version 3.0, 26 July 2016, https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-datamgt_en.pdf

1.4 RELATION TO OTHER TASKS

This report is directly related to all tasks concerning ethics requirements (mainly research and data gathering). The **ENCODE** Coordinator, **ASM**, leads these efforts, having prepared and delivered previous report regarding the processing of personal data, and is about to prepare a report dealing with the ethical requirements. These reports, together with the present one on data management, address ethical and legal issues and are complementary to each other with some content being copy pasted (2.3, 2.4, 2.5) to keep the reports if possible as a stand-alone document. It is important to note that basic information on data management in the **ENCODE project** has already been covered in the **Personal Data Management Plan** report, and this document will fill in any missing details, particularly related to research data.

2 PROCEDURES FOR DATA MANAGEMENT IN ENCODE PROJECT

2.1 DATA COLLECTION

In order to fulfil the objectives, the project will gather a variety of data through multiple research methodologies, each contributing to a comprehensive analysis of emotional and political dynamics. Below are the types of data that will be collected throughout the project:

1. Social Media Data

ENCODE will conduct sentiment analysis to evaluate how social media platforms reflect public emotions on key political topics, such as the COVID-19 pandemic, the Russian invasion of Ukraine, and EU-related policies. Social media data will be collected using search queries based on language-specific keywords tied to the project's theoretical framework. The data extraction process will make use of APIs from platforms like Facebook and Twitter (X), enabling the capture of large volumes of relevant social media conversations. These conversations will be filtered, coded, and analysed to map emotional trends and their relation to democratic processes.

2. Survey Data

ENCODE will deploy comprehensive surveys targeting European citizens, policymakers, and marginalized groups to capture a broad spectrum of emotional responses to democratic resilience and policy-making. The surveys will include validated questionnaires designed to assess the emotional and cognitive responses of individuals to political issues. In particular, the surveys will examine attitudes toward populism, conspiracy theories, and European identity.

3. Interview Data

In-depth qualitative interviews will be conducted with key stakeholders, including policymakers, citizens, and activists. These interviews will explore emotions related to political events and policies, seeking to understand how emotional narratives influence decision-making processes. The interviews will be transcribed and coded to ensure the anonymity of participants while retaining the richness of emotional content.

4. Biometric Data

To complement survey and interview data, biometric research will be conducted. ENCODE will use face-tracking technologies and other biometric methods to capture non-verbal emotional responses during experiments. This data will allow researchers to identify discrepancies between verbal declarations and emotional reactions, providing a deeper understanding of affective political responses.

5. Experimental Data

ENCODE will run a series of experiments involving approximately 2,900 citizens from different European countries. These experiments are designed to observe emotional reactions to various political stimuli, including democratic resilience under stress, and how

7

emotions influence political actions. The data from these experiments will be crucial in developing emotional maps and understanding how emotions shape political behaviour.

6. Heat Maps and Time Series Data

The project will produce heat maps to visualize emotional trends in relation to democratic resilience. These maps will be based on the survey and experimental data collected over time. Additionally, time-series data will be gathered to track the evolution of emotional responses to key political events, providing insights into how emotions fluctuate during crises such as the COVID-19 pandemic and the Russian invasion of Ukraine.

7. Sentiment and Emotion Analysis Data

Advanced machine learning techniques will be used to analyse large datasets collected from social media and survey responses. These analyses will provide insights into how emotions are communicated and reinforced within political discourse. By applying Natural Language Processing (NLP) techniques, the project will identify key emotional drivers and trends across various European countries.

8. Policy-Related Data

Finally, ENCODE will collect data related to the policymaking process, focusing on how emotions shape the interactions between citizens and policymakers. This data will help formulate new policy guidelines aimed at addressing the emotional needs of European citizens, ultimately fostering a more resilient democratic environment.

2.2 FAIR DATA PRINCIPLES

The FAIR principles provide rules and criteria to improve (digital) data discoverability and reuse. A summary of the FAIR principles is herein reported, which are defined[2]:

1. Findable

F1. (Meta)data are assigned a globally unique and persistent identifier.
F2. Data are described with rich metadata (defined by R1 below)
F3. Metadata clearly and explicitly include the identifier of the data they describe
F4. (Meta)data are registered or indexed in a searchable resource

2. Accessible

A1. (Meta)data are retrievable by their identifier using a standardised communications protocol
    A1.1 The protocol is open, free, and universally implementable
    A1.2 The protocol allows for an authentication and authorisation procedure, where necessary
A2. Metadata are accessible, even when the data are no longer available

3. Interoperable

8

I1. (Meta)data use a formal, accessible, shared, and broadly applicable language for knowledge representation.
I2. (Meta)data use vocabularies that follow FAIR principles
I3. (Meta)data include qualified references to other (meta)data

4. Reusable

R1. (Meta)data are richly described with a plurality of accurate and relevant attributes
      R1.1. (Meta)data are released with a clear and accessible data usage license
      R1.2. (Meta)data are associated with detailed provenance
      R1.3. (Meta)data meet domain-relevant community standards

Regarding the availability of data, the following content-specific reports have been designated with a "public" status. As a result, these reports will be actively promoted and made accessible to a broad audience. This ensures that key findings and insights generated throughout the project are disseminated widely, fostering transparency, knowledge sharing, and collaboration within the broader research community and among stakeholders. Additionally, these publicly available reports will contribute to the project's goal of enhancing the visibility and impact of its outcomes, ensuring that the data and insights produced are utilized for further research, development, and practical applications.

Table 1 Public content-related deliverables

Del No	Title	Nature	Dissemination level
D2.1	Key ENCODE's concepts and their intersections	R	PU
D2.2	Theories of emotional politics	R	PU
D2.3	Emotion-related drivers of politics	R	PU
D3.1	Overview of the state-of the art	R	PU
D3.2	Detailed methodology of the social networking analyses	R	PU
D3.3	Sentiment analysis	R	PU
D3.4	Catalogue of best practices	R	PU
D4.1	Methodology for the elicitation of emotions	R	PU
D4.2	Generating emotional responses	R	PU
D4.3	Emotional maps	R	PU
D5.1	Emotions and cognitive and learning effects	R	PU
D5.2	Experimentally-validated survey questions	R	PU
D5.3	Proof of concept: democratic resilience	R	PU
D5.4	Emotions and threats to democracy	R	PU
D5.5	Emotions and mobilisation	R	PU
D5.6	Emotions, gender, and intersectionality	R	PU
D6.1	Co-Creation Methodology	R	PU
D6.2	Co-Creation Report	R	PU
D6.5	Summary report of the co-creation evaluation	R	PU
D6.3	Anonymized dataset	DATA	PU
D6.4	Handbook of emotional politics of the future narratives	R	PU
D7.1	Workshops including guidelines and materials	R	PU
D7.2	Policy brief based on the 6 workshops	R	PU
D7.3	Future scenarios and the roadmap for policy recommendations	R	PU

D7.4	Report on Creating the Alumni group	R	PU

The data generated by the ENCODE project will be made accessible through several channels, ensuring broad dissemination and visibility. Primarily, the ENCODE project website will serve as a central hub for accessing the data. In addition, a variety of promotion activities are planned throughout the project's duration, including newsletters, the sharing of results at events and conferences, presentations at project meetings, and dedicated webinars. The project will also produce videos and brochures to communicate findings more effectively, along with professional and scientific publications aimed at both academic and industry audiences.

Throughout the project, ENCODE partners will actively explore different open repositories where the research data can be deposited, further enhancing accessibility and long-term availability of the data. These repositories could include platforms like Zenodo, Figshare, or institutional repositories, ensuring compliance with FAIR (Findable, Accessible, Interoperable, and Reusable) principles.

Regarding the specific research focus on politics and emotions, the ENCODE project presents several opportunities for publishing and sharing results. As an example:

- **Academic journals specializing in political science,** such as *Political Psychology*, *Journal of Politics*, and *European Journal of Political Research*.
- **Journals focused on emotions in social and behavioural sciences,** like *Emotion*, *Journal of Experimental Social Psychology*, and *Emotion Review*.
- **Conferences** such as the *International Society of Political Psychology (ISPP)*, *American Political Science Association (APSA)*, and *European Consortium for Political Research (ECPR)*.
- **Open access repositories** like *SSRN* for preprints, or discipline-specific platforms like *OpenEmotions* for interdisciplinary research on emotions and politics.

2.3 INFORMATION FOR THE PROCEDURES FOR DATA PROTECTION

In the ENCODE project, data protection is ensured through a combination of robust security measures. Databases containing personal data, such as email addresses, will be secured with strong passwords. Access to these databases is restricted exclusively to authorized ENCODE researchers and project managers. Additionally, any results from interviews will be stored under password protection, with responses coded to anonymize identities. The mapping between names and codes will be maintained by the project coordinator in a secure offline environment or on a digital device (MS SharePoint).

All computers storing project data will be safeguarded by login credentials and password protection. These devices will be further protected with up-to-date antivirus software and an activated firewall. For additional security, after periods of inactivity, a screen saver with password reactivation will be enabled to prevent unauthorized access. This requirement applies to all relevant partners.

Beyond these measures, the ENCODE project follows a layered security approach that incorporates encryption, access controls, and continuous monitoring to protect personal data. Data is encrypted both at rest and during transmission, ensuring that unauthorized access is effectively blocked. Access to data is role-based, meaning that only those with explicit authorization can view or process specific categories of information. To enhance security further, regular audits and assessments are conducted to identify and address

potential vulnerabilities. Moreover, as mentioned several times, compliance with GDPR regulations is integral to the project, particularly regarding the rights of data subjects, such as access, rectification, and erasure.

2.4 INFORMATION FOR THE PROCEDURES FOR DATA DESTRUCTION

At the conclusion of the ENCODE project, or when data is no longer needed, a comprehensive process for data removal will be implemented. Databases containing organizational information will be deleted either when partners decide or, at the latest, at the project's end. Since these databases do not include personal data, rigorous procedures are not required. Contact databases will be securely deleted after the project's conclusion. For files containing interview responses, responses will be coded to prevent the identification of companies or organizations. To maintain methodological credibility and allow scientific verification, these coded responses will be stored for an extended period. However, the list connecting specific organizations/respondents to their codes will be deleted once the research phase is complete, or at the latest, by the project's end.

When data is transmitted via email, it will be saved, digitalized, and then removed from mailboxes to prevent unauthorized access. In alignment with ENCODE's data management practices, any remaining records will be securely destroyed using recognized methods such as cryptographic erasure for digital data and physical destruction for paper records. In cases where data must be archived, strict access controls will ensure that only authorized personnel have access. Moreover, participants retain the right to request the deletion of their data, which will result in immediate and irreversible removal from all storage systems.

2.5 DATA PROTECTION OFFICER

Data Protection Officer (DPO) will be appointed from the Project Coordinator's organization, with contact details: iod@asmresearch.pl made available to all data subjects involved in the research. The DPO is responsible for several key functions, including informing project staff of their rights and obligations related to data protection, ensuring that the ENCODE project complies with GDPR and relevant national regulations when processing personal data, and investigating any data protection concerns that arise. The DPO's role also involves monitoring data processing activities, providing guidance on data protection impact assessments, and serving as the primary point of contact for both data subjects and regulatory authorities.

In the event of a data breach, a predefined procedure will be initiated to evaluate and resolve the incident, focusing on assessing risks to the rights and freedoms of affected individuals. Any security incident posing a high risk will be promptly reported to the DPO, who will take all necessary actions to minimize potential harm. Affected individuals will receive timely email notifications detailing the nature of the breach, the type of information compromised, and the steps being taken to address the issue. Additionally, the DPO may offer training materials for project members and stakeholders to ensure ongoing compliance with data protection standards, while also maintaining a clear and efficient channel for reporting any data breaches and implementing corrective measures.

ACRONYM	FULL NAME
D	Deliverable
DPO	Data Protection Officer
EC	European Commission
EASME	The Executive Agency for Small and Medium-sized Enterprises
GA	Grant Agreement
GDPR	General Data Protection Regulation
PC	Project Coordinator
WP	Work Package
TL	Task Leader
DoA	Description of Action
PDMP	Personal Data Management Plan
SES	Socioeconomic status
SQM	Scientific and Quality Manager
PM	Person month
M	Month