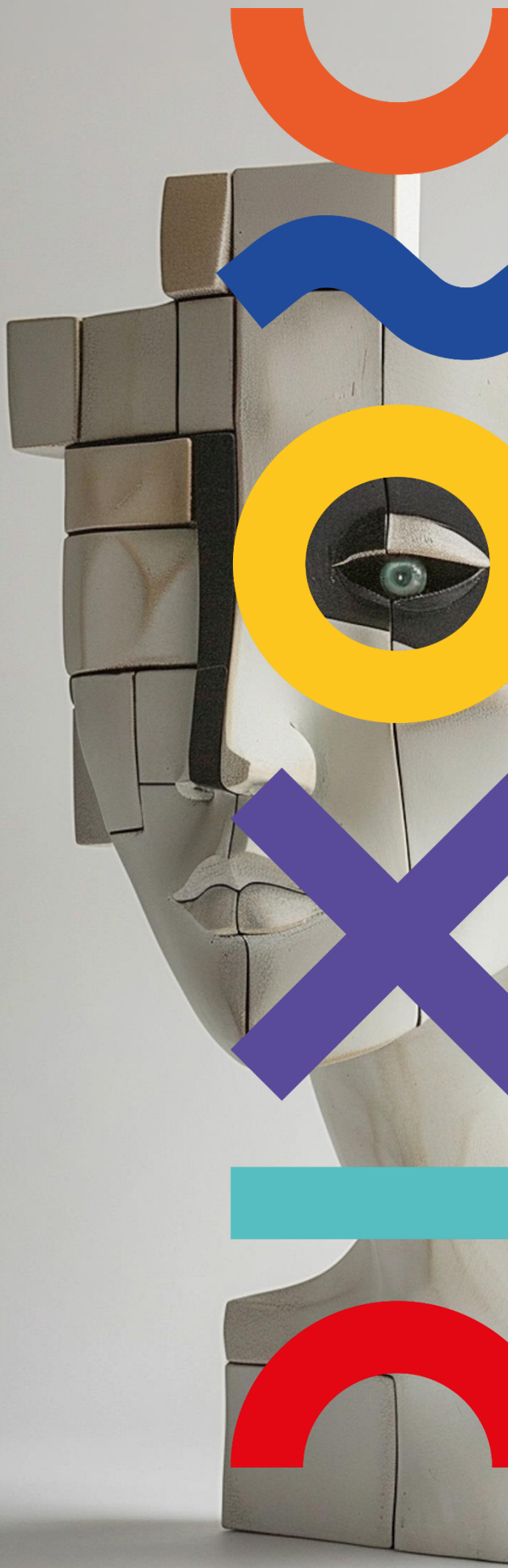
ENCODE

D1.4

Personal Data Management Plan



D1.4 Personal Data Management Plan

Dissemination Level: PU - Public
Lead Partner: ASM
Due date: 31.08.2024
Actual submission date: 31.08.2024

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	25.07.2024	Authors	ASM	Draft
0.2	29.07.2024	Agnieszka Kowalska	ASM	Internal review
0.3	22.08.2024	Łukasz Wilczyński	ASM	Second draft sent to review
0.4	28.08.2024	Seyma Celem	ECPS	Review
0.5	29.08.2024	Łukasz Wilczyński	ASM	Update according to comments
1.0	31.08.2024	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.

Funded by the European Union

This project has received funding from the European Union under the Horizon Europe Research & Innovation Programme (Grant Agreement no. 101132698 ENCODE).

TABLE OF CONTENTS

Funded by the European Union

This project has received funding from the European Union under the Horizon Europe Research & Innovation Programme (Grant Agreement no. 101132698 ENCODE).

EXECUTIVE SUMMARY

The deliverable D1.4 Personal Data Management Plan for the ENCODE project outlines the procedures for data collection, storage, protection, retention, and destruction in line with both national and EU regulations. The primary aim of this document is to ensure that all activities related to data handling within the ENCODE project comply with the highest ethical standards, particularly with regard to the sensitive nature of socio-political research data. This is critical given that ENCODE's focus is on exploring the role of emotions in political engagement and its impact on democratic processes across multiple European countries.

The document provides a comprehensive overview of how data will be ethically managed across various components of the project, including stakeholder databases, which are integral for gathering feedback, dissemination, and communication efforts. Data protection measures are built around the principles of minimization, ensuring that only the necessary data is collected and handled, and the processes are transparent and secure. The procedures involve strict data access controls, regular audits, and secure data destruction methods once the project concludes. Additionally, all project partners are required to follow best practices for data management, which include thorough anonymization and encryption protocols.

Main areas addressed by the document include primary research data handling—ranging from interviews, focus groups, surveys, and biometric data collection—to the secure management of databases containing stakeholder information. Stakeholder engagement is critical to the ENCODE project, as it seeks to bridge the gap between policymakers and citizens by understanding the emotional dynamics influencing political behaviour. These databases support the continuous interaction needed for co-creating emotional narratives and validating strategies for depolarizing political communication.

Funded by the European Union

This project has received funding from the European Union under the Horizon Europe Research & Innovation Programme (Grant Agreement no. 101132698 ENCODE).

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 primary objective of the Personal Data Management Plan (PDMP) is to ensure that all procedures related to the collection, storage, protection, retention, and destruction of personal data within the project are conducted in full compliance with both European and national regulations, including the General Data Protection Regulation (GDPR). The PDMP serves as a comprehensive guideline that outlines how personal data will be managed throughout the project lifecycle.

1.3 STRUCTURE OF THE DOCUMENT

The deliverable is structured in the following sections:

- Chapter 1 - Introduction to the deliverable.
- Chapter 2 – Operating Procedures for Data Management in ENCODE project describes the specific procedures for managing personal data.

1.4 RELATION TO OTHER TASKS

Deliverable 1.4, the Personal Data Management Plan, influences all project tasks involving data collection. This encompasses research activities as well as communication and dissemination efforts.

Funded by the European Union

This project has received funding from the European Union under the Horizon Europe Research & Innovation Programme (Grant Agreement no. 101132698 ENCODE).

2 OPERATING PROCEDURES FOR DATA MANAGEMENT IN ENCODE PROJECT

To start, we would like to formally confirm that all procedures and processes related to the collection, storage, protection, retention, and eventual destruction of data within the ENCODE project, coordinated by ASM, have been carefully aligned with both national and EU legislative standards, including full adherence to the General Data Protection Regulation (GDPR). ASM has diligently adapted its internal protocols to meet GDPR requirements within the required timelines, ensuring that every data-related activity within the project is conducted in a manner that safeguards the privacy, security, and integrity of all collected information.

2.1 INFORMATION ON THE PROCEDURES FOR PERSONAL DATA COLLECTION

2.1.1 RESEARCH PERSONAL DATA COLLECTION

The ENCODE project relies on collecting personal data through various research activities such as surveys, interviews, biometric assessments, and sentiment analysis. The data collected primarily involves demographic details, opinions, emotions, and behaviours related to democratic engagement and emotional responses in the political context. Participants involved in the research activities will be asked to provide explicit informed consent, ensuring transparency about the purpose, scope, and processing of their data. Data collection is structured to align with GDPR and national legal frameworks, ensuring that only the minimum required information is collected, thus upholding the data minimization principle. Procedures are in place to anonymize or pseudonymize data, where applicable, to further enhance participant privacy. Primary data will be gathered in ENCODE project and especially within:

1. WP3 – Analysing Social Media Communication
2. WP4 - Understanding citizens emotional responses – biometrics and qualitative research
2. WP5 – Explaining the effects of emotions
3. WP6 – Active citizen innovation for future narratives
4. WP7 – Forward-looking – foresight and policymaking workshops

What is more, The ENCODE project does not involve handling sensitive data such as health records, genetic information or participant tracking. To ensure the research is conducted efficiently, specific measures will be implemented. To enhance response rates and protect the respondents, some of the interviews will be conducted directly by the responsible project partners in each country. Additionally, all research tools will be translated if needed. This approach also applies to the all online surveys, which will be available primarily in English and widely disseminated. Other project partners will assist by sharing the survey link with their networks and translating the questionnaire and related project information where necessary. Similar all other research techniques will follow that approach, despite biometric research where the assist of ASM will be mandatory.

2.1.2 DISSEMINATION AND COMMUNICATION DATA COLLECTIONS

Funded by the European Union

This project has received funding from the European Union under the Horizon Europe Research & Innovation Programme (Grant Agreement no. 101132698 ENCODE).

Communication and dissemination activities within the ENCODE project will require the processing of personal data. This data may be collected through interactions aimed at gathering feedback on the project or its activities and results. Additionally, personal data will be gathered through subscriptions to the project newsletter and for reaching out to target groups (e.g., to request permission to send newsletters or to invite individuals to project events). As a result, a database containing information such as names, email addresses, institutions, and professional fields will be created to facilitate these communications. Furthermore, the process of registering participants for events or collecting crucial feedback will necessitate the creation of additional databases.

This data will be securely stored on a designated computer at ASM (as coordinator) and ECPS (as communication and dissemination manager) in a password-protected file. The contacts compiled in this database will be used exclusively for dissemination and communication purposes related to the ENCODE project, including sending newsletters, inviting participants to events, and gathering feedback on project developments. Procedures for retaining the data beyond the project's conclusion, as well as protocols for its destruction after a specified period, will be thoroughly detailed to ensure compliance with data protection regulations.

To engage with potential stakeholders and target groups for communication and dissemination, a standardized template will be utilized. The template for requesting consent to send newsletters is as follows:

Subject: Request for Newsletter Consent – European Research Project ENCODE

Dear Sir/Madam,

I hope this message finds you well. I am reaching out to request your permission to send you updates via the newsletter for the European research project ENCODE, conducted under the Horizon 2020 programme. The project aims to drive market-level improvements by providing an operational framework and a suite of services that support the development of a new generation of skilled workers and fitters. Additionally, ENCODE seeks to influence legislative changes that will enhance the demand for energy skills throughout supply chains and across lifecycles.
If you consent to receiving our newsletter, kindly reply with a simple "yes" in response. Should you have any questions, please feel free to reach out to me.

Thank you for your consideration. Your faithfully. XYZ

2.2 INFORMATION FOR THE PROCEDURES FOR DATA STORAGE AND RETENTION

The ENCODE project implements robust and secure storage solutions to ensure the protection of all collected data. Data is stored on encrypted servers (MS Sharepoint) with restricted access, allowing only authorized personnel to handle sensitive information. The storage infrastructure adheres to both EU and national regulations and incorporates best practices in cybersecurity and data management. In line with the principle of data minimization, retention schedules are carefully defined, ensuring that data is retained only for the duration necessary to meet the project's objectives. Following the retention period, data is either securely archived or deleted in accordance with established data destruction protocols.

Databases containing information about organizations relevant for gathering data within ENCODE will be managed by each project partner, with each partner maintaining responsibility for the data gathered, respondents database, etc. in their respective country.

Funded by the European Union

This project has received funding from the European Union under the Horizon Europe Research & Innovation Programme (Grant Agreement no. 101132698 ENCODE).

These databases, which do not contain personal data, will be stored either on computers or in digitalized formats, negating the need for stringent storage procedures.

Contact and stakeholder databases used for communication and dissemination purposes will be, as mentioned above, securely stored on ASM and ECPS computers and will not be shared via digital media or on the project's intranet (e.g., SharePoint).

Data collected during interviews will be stored on computers accessible only by authorized personnel. Once interviews are completed, the recorded data will be securely stored and subsequently removed from the computers once it is no longer needed

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.

Funded by the European Union

This project has received funding from the European Union under the Horizon Europe Research & Innovation Programme (Grant Agreement no. 101132698 ENCODE).

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.

Funded by the European Union

This project has received funding from the European Union under the Horizon Europe Research & Innovation Programme (Grant Agreement no. 101132698 ENCODE).

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

Funded by the European Union

This project has received funding from the European Union under the Horizon Europe Research & Innovation Programme (Grant Agreement no. 101132698 ENCODE).

ENCODE

Funded by
the European Union

This project has received funding from the European Union under
the Horizon Europe Research & Innovation Programme
(Grant Agreement no. 101132698 ENCODE).