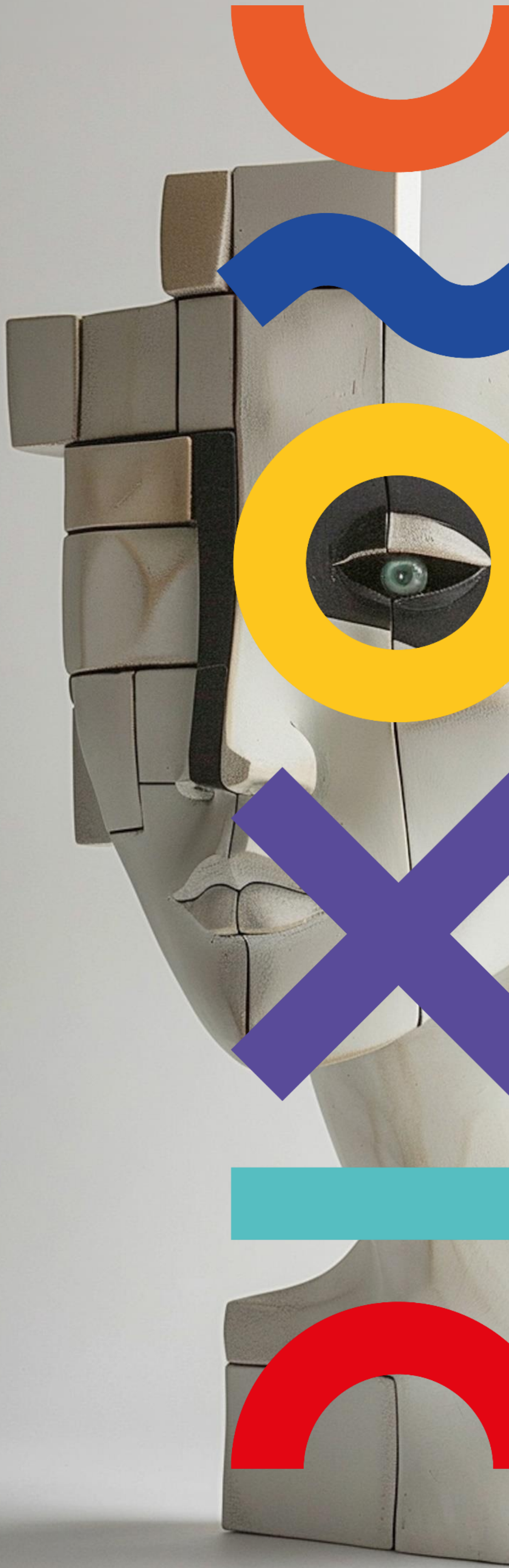
ENCODE

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
Actual submission date after review: 09.01.2026

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
Agnieszka Kowalska, 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
1.1	09.01.2026	Agnieszka Kowalska, Łukasz Wilczyński	ASM	Update according to feedback provided in the 1st review meeting and ENCODE - Review Report
2.0	09.01.2026	Aleksandra Oleksik	ASM	Submission to Participant Portal

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).

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.

All rights reserved

The document is proprietary of the ENCODE consortium members. No copying or distributing, in any form or by any means, is allowed without the prior written agreement of the owner of the property rights.

This document reflects only the authors' view. The European Community is not liable for any use that may be made of the information contained herein. Responsibility for the information and views expressed in the therein lies entirely with the author(s).

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

Deliverable D1.4, the Personal Data Management Plan (PDMP) of the ENCODE project, defines the concrete procedures applied to the lawful and secure processing of personal data throughout the project lifecycle. Complementing Deliverable D1.2 (Data Management Plan), which establishes the general framework for all data types, D1.4 focuses exclusively on personal data and operationalises compliance with the General Data Protection Regulation (GDPR) and relevant national legislation.

The document details how personal data are identified, collected, processed, stored, protected, retained, and destroyed in the context of ENCODE's research, dissemination, and stakeholder engagement activities. It specifies clear workflows, responsibilities, and safeguards applicable across work packages, covering research activities such as surveys, interviews, experiments, biometric studies, and co-creation workshops, as well as communication and dissemination actions involving mailing lists, event registrations, and stakeholder databases. The PDMP applies the principles of data minimisation, purpose limitation, access control, and early anonymisation or pseudonymisation to reduce data protection risks.

The deliverable further describes secure storage arrangements, access controls, retention and destruction procedures, and mechanisms for handling data subject rights and potential data breaches. Oversight is ensured through the appointed Data Protection Officer within the Project Coordinator's organisation, in cooperation with partners' institutional data protection structures. Through these concrete and documented procedures, D1.4 ensures that all personal data processing within ENCODE is carried out transparently, responsibly, and in full compliance with GDPR, thereby safeguarding participants' rights while enabling the effective implementation of the project's objectives.

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. Recognising 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.

Deliverable D1.4 complements Deliverable D1.2 Data Management Plan by focusing exclusively on the management of personal data processed within the ENCODE project. While D1.2 defines the general data management framework applicable to all data types, D1.4 focuses on personal data by detailing concrete procedures for collection, access control, storage, protection, retention, and destruction. The two deliverables are therefore complementary: D1.2 provides horizontal data management rules, whereas D1.4 addresses the specific legal and ethical requirements associated with personal data processing.

1.3 STRUCTURE OF THE DOCUMENT

The deliverable is structured as follows:

- Chapter 1 introduces the deliverable, outlining its scope, objectives, and relation to other project activities.
- Chapter 2 presents the operating procedures for personal data management in the ENCODE project, detailing the concrete processes applied for the collection, storage, protection, retention, and destruction of personal data.

1.4 RELATION TO OTHER TASKS

Personal data management is a cross-cutting requirement that supports all ENCODE tasks involving the collection, processing, or use of personal data. In particular, research activities carried out under WP2, WP3, WP4, and WP5, including surveys, interviews, experiments, social media–based analyses, and biometric measurements, rely on the procedures defined in this Personal Data Management Plan to ensure that personal data are collected, processed, stored, and protected in compliance with GDPR and ethical standards.

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).

In addition, personal data management procedures are essential for participatory and co-creation activities conducted under WP6, WP7 as well as for stakeholder engagement, communication, and dissemination activities under WP7 and WP8, such as event registrations, mailing lists, and targeted outreach. By providing common rules for informed consent, access control, anonymisation or pseudonymisation, secure storage, and data retention, this deliverable enables task leaders across WP2–WP8 to integrate data protection requirements into task planning and implementation from the outset, ensuring consistency, legal compliance, and the protection of participants' rights throughout the project lifecycle.

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 THE ENCODE PROJECT

All procedures related to the collection, storage, protection, retention, and destruction of personal data in the ENCODE project are implemented through operational processes and workflow coordinated by ASM as Project Coordinator and are described in this section.
Compliance with these procedures is monitored through internal checks during Work Package meetings, deliverable reviews, and coordination activities. Where required, institutional Data Protection Officers support partners in applying GDPR-compliant procedures, including consent management, data subject rights, and incident handling.

The operational workflow for personal data management in ENCODE applied across all tasks involving human participants or identifiable information is presented below:

- Identification: At the start of each task, an initial assessment is carried out to determine whether personal data will be collected or processed. Where personal data are involved, the relevant data categories are identified and documented prior to the commencement of data collection activities.
- Collection: Personal data are collected only where necessary for the specific task and based on an appropriate legal ground, such as informed consent. In dissemination and communication activities (e.g. event registrations or mailing lists), personal data are collected solely for clearly defined purposes and processed in accordance with applicable data protection rules.
- Access control: Access is restricted to authorised researchers involved in the relevant task.
- Processing: Data are anonymised or pseudonymised at the earliest possible stage.
- Storage: Personal data are stored on secure institutional servers or protected project platforms.
- Retention and destruction: Retention periods are defined in advance and personal data are securely deleted or anonymised once no longer required.

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, sentiment analysis, Delphi panel and co-creation sessions and workshops. The data collected primarily involves demographic information (e.g. age group, gender, education level), expressed opinions, emotional responses, and behavioural indicators related to democratic engagement and political communication. No unnecessary identifying information is collected beyond what is required for the specific research purpose.

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 minimisation

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).

principle. At the point of collection, personal data are either anonymised immediately or pseudonymised as soon as technically feasible. Direct identifiers are avoided wherever possible and, where used, are stored separately from research data only for the purpose of checking the list of attendance and delivering incentives (they are not connected with the research data itself)

.

Primary data will be gathered in the ENCODE project, and especially within:

1. WP2 - Heightened understanding – a theoretical framework and an empirical review – interviews with policy-makers
2. WP3 – Analysing Social Media Communication – analysis of social media posts
3. WP4 - Understanding citizens' emotional responses – biometrics and qualitative research
2. WP5 – Explaining the effects of emotions - panel surveys, experiments
3. WP6 – Active citizen innovation for future narratives - co-creation workshops
4. WP7 – Forward-looking – foresight and policymaking workshops - foresight workshops

The ENCODE project does not process special categories of personal data such as health records, genetic information, or continuous participant tracking. Research activities are designed to minimise data protection risks while ensuring methodological robustness. Interviews are conducted directly by the responsible project partners in each country, allowing data collection to be carried out in the local language, where necessary, and context and reducing the need for unnecessary data transfers.

Research instruments, including interview guides and survey questionnaires, are translated where required to ensure accessibility and comprehension for participants. Online surveys are prepared in English and, where relevant, translated into additional languages.

The same approach applies to other research methods implemented in the project, with data collection and initial processing carried out at the partner level. An exception applies to panel surveys as well as biometric research activities: face and eye-tracking studies are conducted by ASM in partner countries to ensure methodological consistency and secure handling of biometric data, while in-depth interviews in WP4 are carried out by national partners in the relevant local languages where necessary, in accordance with applicable ethical and data protection requirements.

2.1.2 DISSEMINATION AND COMMUNICATION DATA COLLECTION

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.

The contacts collected 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.

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).

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

Subject: Request for Newsletter Consent – European Research Project ENCODE

Dear Sir/Madam,
We are contacting you in the context of the ENCODE research project, funded under the Horizon Europe programme, which studies the role of emotions in political engagement and democratic processes.
We kindly ask for your consent to receive information about project activities, events, and results (e.g. newsletters or invitations). Your personal data will be processed solely for communication and dissemination purposes related to ENCODE and in compliance with the General Data Protection Regulation (GDPR).
You may withdraw your consent at any time.
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.
Yours faithfully, ENCODE team

2.2 INFORMATION FOR THE PROCEDURES FOR DATA STORAGE AND RETENTION

The ENCODE project applies secure storage procedures for all personal data collected in the course of research, communication, and dissemination activities. Storage solutions are selected based on data sensitivity, access requirements, and applicable legal obligations, ensuring compliance with the GDPR and relevant national legislation.

.

Personal data are stored on secure institutional servers operated by the respective consortium partners or, where appropriate, within the protected ENCODE project SharePoint environment, managed by ASM. These storage environments implement technical and organisational safeguards, including encryption, restricted access rights, and authentication mechanisms, ensuring that personal data are accessible only to authorised project personnel with a legitimate role in the relevant task.

Databases containing contact details of organisations or individuals involved in ENCODE research activities are maintained by the responsible project partners at the national level. Each partner remains responsible for the secure storage and protection of personal data collected within its country, including respondent contact lists and consent records. Access to such databases is limited to authorised staff, and personal data are not transferred or shared beyond what is necessary for project implementation.

Audio recordings or raw interview materials are stored separately from processed or anonymised research data and are deleted or anonymised once transcription, validation, and quality checks have been completed, unless a longer retention period is justified and documented.

.

Contact and stakeholder databases used for communication and dissemination purposes are stored securely on the ENCODE project's protected SharePoint environment, managed by ASM, as well as on the institutional servers of ECPS or project Partners, where necessary, in a password-protected file. These databases include contact details of individuals who have explicitly agreed to be contacted in the context of the ENCODE project, as well as publicly available professional contact information collected from institutional or organisational websites.

The databases are developed progressively, starting with contacts available at EU level identified by ECPS, followed by contacts provided by consortium partners from their professional networks and publicly accessible national sources. Access to the databases is restricted to authorised staff involved in ENCODE activities, and personal data are processed

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).

exclusively for project-related communication purposes, in accordance with applicable data protection requirements.

2.3 INFORMATION FOR THE PROCEDURES FOR DATA PROTECTION

In the ENCODE project, personal data protection is ensured through a combination of organisational and technical measures applied consistently across all tasks involving the processing of personal data. These measures are aligned with the GDPR and complement the general data security framework described in Deliverable D1.2, with a specific focus on safeguarding personal data.

Access to personal data (e.g. contact details, interview materials, survey responses, biometric indicators) is restricted to authorised project staff who require such access for the execution of their tasks. Personal data are protected through access controls and authentication mechanisms, ensuring that only designated researchers or project staff can view or process specific categories of personal data.

Personal data stored in digital form are protected through password-secured user accounts on institutional servers or the ENCODE project's protected SharePoint environment. Devices used for processing personal data are safeguarded by individual login credentials, up-to-date antivirus software, activated firewalls, and automatic screen-lock mechanisms after periods of inactivity. These requirements apply to all partners processing personal data within the project.

To reduce identification risks, personal data collected during research activities are anonymised or pseudonymised at the earliest possible stage. Where pseudonymisation is applied, identifiers are replaced with codes, and any correspondence between identifiers and codes is stored separately under restricted access by the responsible partner.

In line with the layered security approach defined in D1.2, personal data are protected through encryption and/or passwords during storage and transmission, as well as through regular internal checks to ensure that access rights and security measures remain appropriate. Detailed cybersecurity procedures are described in D1.2 and apply equally to personal data processed in ENCODE.

Compliance with GDPR also includes respect for data subject rights, including the right of access, rectification, restriction of processing, and erasure. Requests from data subjects are handled in coordination with the appointed Data Protection Officer, in accordance with the procedures outlined in Section 2.6 of this deliverable.

2.4 INFORMATION FOR THE PROCEDURES FOR DATA DESTRUCTION

Personal data processed within the ENCODE project are retained only for as long as necessary to fulfil the specific purpose for which they were collected. At the conclusion of the project, or earlier where personal data are no longer required, defined procedures are applied to ensure the secure and irreversible destruction/deletion or anonymisation of personal data.

Personal data contained in contact and stakeholder databases used for research, communication, or dissemination purposes are securely deleted once they are no longer needed, and at the latest by the end of the project, unless a longer retention period is justified and documented.

For research data derived from interviews, surveys, or other qualitative methods, identifiers are removed or replaced with codes at an early stage. Any lists or files linking personal identifiers to coded research data are stored separately under restricted access and are deleted once the research phase requiring identification is completed, or at the latest by the

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).

end of the project. Coded or fully anonymised research data may be retained for a longer period for scientific validation or reuse, provided that re-identification is no longer possible.
Personal data transmitted electronically during the project (e.g. via email) are transferred to secure storage environments as soon as possible and subsequently removed from mailboxes to reduce the risk of unauthorised access. Personal data stored on local devices are deleted once they have been transferred to the designated secure storage or once they are no longer required.
Secure destruction of personal data is carried out using recognised methods appropriate to the storage medium, such as cryptographic erasure or secure deletion for digital data and physical destruction for any paper-based records using paper shredder. Where anonymised data are archived for scientific purposes, strict access controls apply to ensure that only authorised personnel can access the data.
In accordance with the GDPR, data subjects retain the right to request the deletion of their personal data. Such requests are handled without undue delay and result in the irreversible removal of the relevant personal data from all storage systems, unless retention is required by law or justified for overriding research purposes in accordance with applicable regulations.

2.5 DATA PROTECTION OFFICER

For the ENCODE project, data protection oversight related to the processing of personal data is ensured through the appointment of a Data Protection Officer (DPO) within the Project Coordinator's organisation (ASM). The DPO (Katarzyna Walburg) can be contacted at iod@asmresearch.pl, and these contact details are made available to all data subjects involved in ENCODE activities as well as on the ENCODE project website. Moreover, for research activities involving participants, information on the project is accompanied by contact details of the relevant partners' institutional Data Protection Officers, enabling participants to communicate in their local language where appropriate.

Within the scope of this Personal Data Management Plan, the DPO supports the lawful and compliant processing of personal data by advising the Project Coordinator and consortium partners on their obligations under the General Data Protection Regulation (GDPR) and applicable national legislation. In particular, the DPO provides guidance on personal data collection practices, consent management, data minimisation, retention periods, and the handling of data subject rights in the context of ENCODE research and dissemination activities.

The PC and DPO monitor personal data processing activities related to the project and acts as a point of contact for project partners when questions or concerns arise regarding the protection of personal data. Where required, the DPO provides advice on data protection impact considerations for specific research activities involving personal data.

In the event of a personal data breach, partners are required to inform the Project Coordinator without undue delay. The Project Coordinator, in coordination with the DPO, assesses the incident and determines the appropriate response, including whether notification to the relevant supervisory authority and affected data subjects is required. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, affected data subjects are informed in a timely manner, in accordance with GDPR requirements.

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
DoA	Description of Action
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
PDMP	Personal Data Management Plan
PC	Project Coordinator
WP	Work Package

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).