Proposal Acronym:
DATIS

Proposal Title:

Data for Inclusive Societies: Foes and Friends of Inclusiveness in contemporary Greece

D1.2: Data Management Plan Final Version

December 2025

Introduction

This report provides an overview of the data management strategy of the project. Focusing, therefore, on the data management policy (data collection procedures (i) the methodology that was applied in terms of data collection and quality assurance procedures, (ii) the usefulness of the data, and (iii) the procedures followed sharing, protection and retention of the data in the end of the project. This is the final version of the data management strategy of the DATIS project.

Data Collection and Quality Assurance Procedures

The DATIS project draws on the completed datasets from the European Parliament (EP) 2024 (candidates' and voters' surveys), the ISSP 2024 module on citizens' attitudes towards Digital Societies, as well as the completed pilot survey on inclusive societies. The main DATIS survey on inclusive societies has been implemented together with the ISSP 2025 module on Work Orientations from May to July 2025. In addition, the extension of the EP candidates as a survey of political elites and the survey experimnents on issues related to social inclusion, exclusion, and inequality in the digital age has also been carried out and is now fully integrated into the broader research framework of DATIS.

The data collected within the project address issues of inclusion and exclusion of minority groups in social and political life, citizens' attitudes towards the European Union, and the degree of inequality emerging from the expansion of the Internet and digital technologies. This data falls into two categories: a) survey data (candidates, voters), b) data from social media posts (META).

The surveys (European Parliament 2024, ISSP 2024, DATIS pilot survey, DATIS main survey, DATIS survey experiments, DATIS political elites survey) were conducted through "LimeSurvey", an open access software for online surveys. Survey data was also extracted from the same software. From the initial design of the surveys, each participant was given a specific "token", so as to ensure that the survey was completed by only one participant. Then, once the data has been collected, data cleaning methods were applied based on response quality indicators such as item-nonresponse, time spent on each response, etc.

The use of data

DATIS data is useful, both to scientists and to society and business. Overall, all project data and its analysis contributed to making it available valuable scientific knowledge about the two political phenomena under consideration in society.

The dissemination of scientific knowledge to society and in particular information related to contemporary political phenomena contributed to a better representation of citizens, who, knowing better the positions of political parties and candidates on various social and political issues. In addition, since the data is freely accessible to scientists, it also strengthened scientific research. More specifically, DATIS data is used by social scientists, by data scientists, by those -scientists and non-scientists- engaged in online research, etc.

General Data Protection Regulation (GDPR)

Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 establishes the new General Data Protection Regulation in the European Union. The new regulation establishes strict rules regarding the collection, processing and storage of personal data of European Union citizens. These include individuals, companies, public or non-governmental organizations. The General Data Protection Regulation (GDPR) was approved on 27 April 2016 and came into force on 25 May 2018 after a two-year transition period.

However, the legal interpretation of the term "personal data" is quite broad as it is data related to the individual and concerning information, both about their personal, professional and public life, which, if collected together, can lead to their identification. For example, such information is: name, home address, email address, Internet Protocol (IP) address etc.

According to the General Data Protection Regulation, data collection can only start after the respondents have clearly expressed their consent. The respondents must also be clearly informed about the data being collected and for what purpose. After being informed about the type and purpose of the data, the time of their retention and the way they can exercise their rights, they must expressly agree to the collection of the data. This is ensured through the consent the participants give at the beginning of each survey. Only after they give their consent, do they start answering the survey. In case they do not agree, the survey is terminated immediately and they are informed that they cannot complete the survey, due to their objection to the collection of their data.

The respondent had the right to withdraw consent at any time. Withdrawal of consent does not affect the lawfulness of processing that was based on consent prior to its withdrawal. In any case and at any time, the respondent had the right to access, correct and delete (right to be forgotten) personal data, to limit their processing, to oppose their processing and to their portability.

Furthermore, according to the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (Article 8, Paragraph 1) the processing of a child's personal data is lawful only if the child is at least 16 years old. If the child is under the age of 16, such processing is lawful only if and to the extent that such consent is given or approved by the person having parental responsibility.

When personal data is collected, the controller provides the data subject with the following information: his/her identity and contact details of the data controller (and the personal data protection officer, if any), the purposes of the processing for which the personal data is intended and the way of exercising his rights.

Data Protection

The data that was collected during the project takes two forms: a) publicly available data and b) personal data (data of a personal nature). Regarding the collection of personal data there was full compliance with the General Data Protection Regulation (GDPR). More specifically, in all surveys that were conducted by the project's research team - both online and over the phone –

at the beginning of the surveys there was a consent form, which included information about the purpose of the research, ensuring anonymity and the rights of the participants, while informing them that their participation in the research was optional and they could interrupt it at any stage of conducting the investigation.

In addition, in surveys addressed to voters, there was a question that appeared after the respondents had given their consent for recording, storing and statistical processing of their responses, asking respondents if they were under 16 years old. If the respondents answered that they were under 16 years old, they were automatically excluded from the survey as according to Article 8(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. They could not participate in investigations without the consent of a guardian.

In terms of ensuring anonymity, voter survey data could not easily lead to the identification of participants, as the technique of generalization was adopted. Additionally, since the invitations to participate in the voter surveys were sent to mobile phone numbers, it is necessary to clarify that the mobile phone numbers were randomly generated by a computer algorithm (RDD – Random Digit Dialing) and therefore it was not possible to associate a number with its owner. Invitations to participate in the surveys to randomly selected numbers were sent using the infrastructure of a private company specialized in sending text messages. It is worth noting that there is no connection between the mobile phone numbers and participants' responses. Mobile phone numbers were kept separately from survey responses so that there was no link between survey responses and mobile phone numbers. The mobile phone numbers of the participants together with the link included in the invitation, were on the server of the company that was used to send the text messages and they were deleted after the sending process was over. These are highly secure servers and the only way to extract information that could link a mobile phone number with a specific response in the surveys is if both servers were hacked during the period of data collection. However, if any problem occurs on one of the two servers, the other was automatically informed and stronger measures were taken.

In addition, the voter surveys meet the requirements of the current AUTH Code of Ethics and all participants in the surveys were informed about surveys' purposes. Sample members were invited to a website, where they could find information about the personal data protection policy, the rights of the participants and how to exercise them, as well as the contact information of the data controller and the scientific manager of the project.

Ethical Issues META

In the context of this project, all the necessary measures had been taken to ensure the anonymity of the research participants and the protection, in accordance with the GDPR (General Data Protection Regulation), of their sensitive personal data. In particular, with regard to ensuring anonymity in the specific research that includes the collection of data from social media posts, which concern publications (posts) of European Elections 2024 candidates and parties on pages or groups on Facebook and Instagram, is detailed in article 28 of Law No. 4624/2019 regarding the reconciliation of the right to the protection of personal data with the right to freedom of expression and information, including processing for journalistic purposes and for purposes of academic, artistic or literary expression.

According to this law, the processing of personal data is permitted, when the right to freedom of expression and the right to information prevail over the right to protect the subject's personal data, in particular for matters of general interest or when it concerns the personal data of public figures.

Data Storage and Retention

All the data of this project were stored in an encrypted form on the server of the scientific manager and will be kept for at least five years after the end of this project. At the same time, the anonymized data are published on the project website (http://datis.gr/) where they will remain available for the same period of time. Survey data will also be stored in online open access repositories such as Zenodo, in order to facilitate their wider dissemination and use.

Data Sharing

All DATIS survey data is open access data. Survey data are published on the project website (http://datis.gr/) and later they will be available in data repositories (e.g. Zenodo: https://zenodo.org/).