Plan Overview

A Data Management Plan created using DMPonline.be

Title: Democracy Paradox

Creator: Joachim Waterschoot https://orcid.org/0000-0003-0845-9310

Affiliation: Ghent University (UGent - UZ Gent)

Template: Faculty of Psychology & Educational Sciences DMP +

Principal Investigator: Joachim Waterschoot https://orcid.org/0000-0003-0845-9310

Data Manager: Joachim Waterschoot https://orcid.org/0000-0003-0845-9310

Project Administrator: Joachim Waterschoot https://orcid.org/0000-0003-0845-9310

Project abstract:

The trend towards more democratic governance across the world stands out as an indicator of the progress in human development during the 20th century. Although democracy has benefits for society at large and for citizens' individual mental health, the 21st century has globally witnessed a tendency of democratic backsliding and growing support for autocratic alternatives. This proposal, grounded in Self-Determination Theory, seeks to unravel this paradox by investigating the role of citizens' basic psychological needs for autonomy, relatedness, and competence, both at the individual and group-based level. A central hypothesis is that the satisfaction and frustration of these needs explain 'why' democracy enhances mental health and, at the same time, 'when' and for 'whom' autocratic alternatives gain appeal. When confronted with societal threats, particularly people with more experiences of need frustration would lose faith in democracy and favor autocratic governance instead. The project consists of three interconnected work packages: (1) a cross-national study involving 60 countries (2) a 3-wave longitudinal study allowing to examine the hypotheses at the level of change across time, and (3) an experimental study exposing participants to standardized threats. Through this multi-method approach, this project aims to illuminate the paradoxical situation of democracy in the 21st century, with citizens turning away from a political regime that is beneficial for their well-being.

ID: 217479

Start date: 01-08-2025

End date: 12-11-2029

Last modified: 09-01-2026

Grant number / URL: BOF/PDO/2025/011

Collection and processing of personal data

1. Are you collecting or processing personal data?

- Yes

The study collects anonymous survey data that may include sociodemographic variables such as age, gender, and country of residence. These survey data are anonymous from the moment of collection and do not constitute personal data under GDPR.

In addition, participants may optionally provide an email address solely for the purpose of being contacted for a possible follow-up study. Email addresses constitute personal data and are collected via a separate step, stored separately from the survey data within the secure Ghent University environment, and are never shared with research partners or included in analytical datasets.

2. In what format are you collecting or processing the personal data?

- Digital

Digital only. Personal data are collected exclusively via a secure online questionnaire (Qualtrics) and stored in digital formats (e.g., CSV/SPSS/R formats) on UGent-managed infrastructure. No paper-based surveys are used in this project, in order to guarantee a uniform anonymity and data-protection procedure across all participating countries.

3. Are you collecting or processing primary personal data and/or secondary personal data?

- Primary personal data

The study will collect personal data directly from participants for the specific purposes outlined in the research protocol, primarily through online surveys administered via a secure web-based platform (Qualtrics). No paper-based surveys are used in this project. These data will be obtained with informed consent and processed in compliance with GDPR. No secondary personal data from external sources will be used.

4. If you are processing secondary personal data, will you inform the persons whose personal data are being processed or have they already been informed?

- No

The study will not process secondary personal data; all personal data will be collected directly from participants as primary data with informed consent.

5. If no, explain why it is impossible or why it would take a disproportionate effort to inform the persons whose personal data are being processed.

Not applicable, as no secondary personal data will be processed in this study. All personal data will be collected directly from participants with informed consent.

6. How will the personal data be processed?

- Pseudonymised (explain below)

- Anonymised (explain below)

Survey data are collected fully anonymously. No IP addresses, metadata, geolocation data, or direct identifiers are collected, and Qualtrics IP logging is disabled.

Optional re-contact (UGent only): Participants may voluntarily provide an email address for follow-up surveys. These email addresses are stored separately and linked to an internal UGent-only participant code for re-contact purposes. This pseudonymisation applies only to the contact data, not to the survey data.

Any data shared outside Ghent University are fully anonymised and do not include contact information, internal participant codes, or longitudinal linkages.

7. If you are going to process personal data in a pseudonymised form, describe the method of pseudonymisation, where you will keep the key, and who has access to it.

Pseudonymisation applies only to participants who voluntarily provide an email address for optional follow-up. In that case, the email address is linked to a randomly generated UGent-internal pseudonymised participant code.

The key file linking email addresses to pseudonymised codes is stored separately from the research dataset on a secure UGent server with access control. Access to this key file is restricted to the principal investigator (and, where necessary, authorised UGent researchers for operational follow-up purposes).

Local research partners and external collaborators never have access to the key file, the email addresses, or the UGent pseudonymised codes. When data are prepared for external sharing, UGent pseudonymised codes are removed and replaced by newly generated anonymised random codes. Also, sociodemographical variables are oversimplified to make sure participants' specific sociodemographic profile is not traceable.

Categories of personal data & data subjects

8. Are you collecting/processing any of the following special categories of data?

- Data on psychological and mental health
- Data about a person's sex life or a person's sexual orientation
- Data on physical health
- Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union memberships

The survey will include questions on participants’ perceptions of democracy and attitudes toward political systems; questions on self-reported mental health; validated measures of psychological well-being and ill-being; and optional questions on sexual orientation and relationship status, which may relate to a person’s sexual orientation. All such data will be collected only when essential for the research objectives, handled in compliance with GDPR, and anonymised before analysis and sharing to minimise any risk of re-identification.

9. Which other categories of personal data are you collecting/processing?

- Identification data (names, titles, addresses, phone numbers, passport numbers, IP addresses, cookies, electronic location data (GPS, mobile phone)…)
- Household composition; family membership
- Occupation and profession
- Age
- Sex
- Marital status
- Nationality
- Ethnicity

The questionnaire collects anonymous sociodemographic and attitudinal data.
Optional: email address (only if the participant explicitly consents to being re-contacted for a follow-up wave).

10. Whose personal data are you collecting/processing?

- Healthy persons

The study will collect personal data from adult participants (aged 18 and above) residing in participating countries across different world regions. Participants are recruited exclusively via online channels through survey links disseminated by local research partners. No personal data will be collected from minors or vulnerable populations unless explicitly approved by relevant ethics committees and accompanied by additional safeguards.

11. Will your research be seriously hampered if the persons whose personal data are being collected/processed exercise their right to access, to rectification, to restriction of processing, to be forgotten, to data portability and/or to object?

- No

Participants may stop at any time before submitting the questionnaire by closing the browser window. Because questionnaire responses are collected anonymously (no direct identifiers and IP logging disabled), individual questionnaire submissions cannot be retrieved or deleted after submission. This limitation is clearly communicated in the informed consent.

For participants who optionally provide an email address for follow-up contact, data subject rights (e.g., deletion of contact details) can be exercised with respect to the email address record. Participants can request removal of their email address from the re-contact list at any time.

12. If yes, please justify the need to deviate from one or more of the rights mentioned in question 11. A justification is required for each deviation.

Since the answer is **No**, no deviation from the rights mentioned in question 11 is required, and full compliance with all applicable GDPR rights will be maintained.

Purpose(s) of the processing

13. What is/are the purpose(s) of the personal data processing?

The purpose of processing personal data is to investigate the psychological mechanisms linking perceptions of democracy to well-being and ill-being across different countries and contexts. Specifically, the data will be used to examine how basic psychological needs (autonomy, relatedness, competence), physical and mental health, and socio-demographic factors relate to individuals' democratic perceptions and political attitudes. Processing these data is essential for answering the research questions, conducting cross-national comparisons, testing theoretical models from Self-Determination Theory and political psychology, and producing scientific publications and presentations based on aggregated, anonymised results.

14. What is the legal ground for the processing? If the data are being processed for multiple purposes, you must describe the legal ground for each purpose.

- The individuals participating in the research have freely given their explicit consent for the processing of their personal data for one or more specific purposes.

Participation will be entirely voluntary, and informed consent will be obtained prior to data collection. The consent form will clearly explain the study's purpose, the types of personal data collected, how these data will be processed and stored, the rights of participants under GDPR, and how anonymised data may be shared for scientific purposes.

15. If you are processing special categories of personal data (see question 8), on which exception is this based?

- The data subject has given his or her explicit consent.

Special categories of personal data will only be collected when essential for the research objectives, and participants will provide explicit consent for their collection and processing. The consent process will clearly explain the nature of these data, the purpose of their use, and the measures taken to ensure confidentiality and compliance with GDPR.

GDPR responsibility

16. Which institution(s) is/are involved in the research?

- Ghent University

17. Is there another university, hospital, research institute or partner involved in the research (besides Ghent University and/or Ghent University Hospital)? If yes, specify below.

- Yes

The research involves multiple international partner institutions, including universities and research institutes in participating countries across different world regions (63 countries including 125 researchers who had given consent and signed engagement for collaborating on this study). Each partner is responsible for local data collection in accordance with the harmonised study protocol (i.e., sharing sufficient amount of participants via a link provided by Ghent University team), GDPR, and any applicable national regulations. Via a digital online dashboard, only available for collaborators, they can check updates on the number of completed surveys in their corresponding country. Data is not transferred as this is saved directly on server of Ghent University for integration and analysis.

18. Please specify who determines the purposes ('why') and the means ('how') of the research.

- This is determined within Ghent University: UGent is the data controller.

Data transfers & categories of recipients

19. Are you disclosing/sharing/transferring personal data beyond your project team, either with recipients in UGent or UZ Gent, or with external recipients during or after your research?

- Yes

No personal data (e.g., email addresses) are shared beyond the UGent project team.
For scientific collaboration, only fully anonymised and simplified cross-sectional datasets (single wave) are shared with external collaborators. These datasets do not contain contact information, do not contain UGent pseudonymised codes, and are processed to prevent re-identification (e.g., categorisation, collapsing small cells, suppression of rare combinations).

20. If yes, to or with which categories of recipients are the personal data being disclosed/shared/transferred?

- Other researchers within your department
- Other researchers outside UGent or UZ Gent

Not applicable for personal data. Email addresses and linkage information remain within UGent. Only anonymised cross-sectional research datasets may be shared with external academic collaborators for scientific purposes.

21. If yes, where are the personal data being disclosed/shared/transferred to?

- Belgium
- Another country within the European Economic Area (EEA) (please specify the country below)
- A country outside the European Economic Area (EEA) but on the European Commission’s ‘white list’ (please specify the country below)
- A country outside the European Economic Area (EEA) and not on the ‘white list’ (please specify the country below)

No personal data are shared with partner institutions.
Only fully anonymised, cross-sectional survey datasets are shared for scientific collaboration.

22. What is/are the purpose(s) of the data transfer?

The purpose of the data transfer is to facilitate the secure collection, consolidation, and analysis of anonymised survey data from all participating countries. While local partner institutions coordinate participant recruitment and oversee practical aspects of data collection, all responses are entered directly into the secure online survey platform managed by Ghent University via a shared survey link. This ensures that Ghent University receives the data in real time, enabling immediate quality control, harmonisation of variable coding, and integration into the international dataset for cross-national analysis. Data access will be limited to authorised researchers, and all processing will be conducted in compliance with GDPR.

23. What is the legal ground for the data transfer? If there will be multiple data transfers, you need to indicate the legal ground for each data transfer.

- The individuals participating in the research have freely given their explicit consent for the transfer of their personal data for one or more specific purposes.

Participants are informed that anonymised survey data may be shared securely with collaborating researchers for scientific purposes.

Retention period

24. What is the envisaged retention period for the different categories of personal data? Please motivate.

Identifiable personal data (e.g., contact details collected solely for longitudinal follow-up) will be retained only for as long as necessary to complete the follow-up phase and will be deleted within 12 months after the final follow-up contact. Anonymous research data will be retained for the duration of the project and subsequently preserved in anonymised form for long-term scientific use.
The anonymised dataset, along with accompanying documentation, will be preserved for a minimum of 10 years after project completion in accordance with Ghent University’s research data management policy and funding body requirements, to allow for verification, secondary analyses, and potential meta-analyses.
All retention will comply with GDPR, and appropriate security measures will be in place throughout the storage period to protect personal data from unauthorised access or loss.

Risk analysis

25. To analyse the possible risks associated with the processing of personal data, please tick the boxes that apply to this research.

- Special categories of personal data are processed in this research (see question 8).
- Personal data are processed on a large scale (please consider the number of data subjects concerned, either as a specific number or as a proportion of the relevant population).
- Aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements are evaluated or scored, profiled or predicted.
- The data are transferred beyond the borders of the EU or the EEA, or to a country not listed on the ‘white list’ (see question 21).

- The research involves datasets that have been or will be matched or combined.

This research involves **special categories of personal data** (political opinions, physical health, psychological and mental health, sexual orientation or sex life), and **personal data processed on a large scale** (thousands of participants across multiple countries). It evaluates **aspects concerning participants' health, personal preferences or interests, reliability or behaviour** (e.g., well-being, psychological needs, political attitudes), and **transfers data beyond the borders of the EU or the EEA, including to countries not on the 'white list'** (see list in question 21). In addition, **datasets will be matched or combined** (e.g., merging country-level indicators from third-party sources with individual survey data).

26. Does the research constitute a probable high-risk processing? If you ticked two or more boxes in question 25, the answer is 'yes'.

- Yes

Multiple high-risk criteria from question 25 apply, including the processing of special categories of personal data, large-scale processing, evaluation of aspects related to health and personal preferences, international data transfers to non-white-list countries, and the combination of datasets. These factors together constitute probable high-risk processing under GDPR.

Security measures

27. What technical and organisational security measures are in place to protect personal data?

- I hereby confirm that I carry out my research in accordance with the guidelines on information security of UGent and/or UZ Gent.
- Additional security measures will be or have been taken (please specify below)

Survey data are anonymous from the moment of collection. Pseudonymisation applies only to optional contact data for follow-up, which are stored separately in encrypted files with restricted access.

28. If you have motivated the need to deviate from one or more of the rights of the persons whose personal data you are collecting/processing in question 11 and 12, please describe which safeguards are put in place to protect their rights and freedoms.

No deviation from the rights of the persons whose personal data are being collected or processed has been motivated in questions 11 and 12. Therefore, all applicable GDPR rights will be fully respected, and standard safeguards, such as informed consent, the right to withdraw, pseudonymisation, secure storage, and controlled access, will be applied to protect participants' rights and freedoms.

Administrative Data

Date of first version

August 14, 2025

Date of last update

Jannuary 9, 2025

1. Data Collection

1.1 What data will you collect or create?

We will collect **quantitative survey data** on participants' perceptions of democracy, basic psychological need satisfaction and frustration, well-being and ill-being indicators, and socio-demographic characteristics. Data will be stored primarily in non-proprietary formats (CSV) alongside R (.RData) formats for analysis, with documentation in PDF (e.g., questionnaires, consent forms) and XLSX (e.g., codebooks, variable lists). The final dataset, covering multiple countries, is expected to total approximately 1-2 GB. These formats are standard in social science research, compatible with widely used statistical software, and suitable for long-term usability and interoperability. In addition, publicly available third-party datasets containing objective country-level democracy indicators and socio-economic statistics (e.g., Freedom House, World Bank) will be integrated, with full citation and use limited to openly accessible data.

1.2 How will the data be collected or created?

Data will be collected via **an online survey** using standardized questionnaires based on validated measures from Self-Determination Theory and political psychology research. The survey will be hosted on **a secure platform** (e.g., Qualtrics) and will follow common data capture standards in the social sciences, including pre-testing, consistent item wording, and standardized response scales. Each participating country will be provided a harmonized protocol for recruitment, informed consent, and data collection to ensure comparability across sites. Data files will be organized using a hierarchical folder structure separating raw data, cleaned datasets, syntax files, and documentation. File naming will follow a consistent convention including country code and date. Version control will be maintained through Git for analysis scripts and by keeping archived, read-only copies of each dataset version, allowing retrieval of earlier versions if needed. Quality assurance will include automated data checks in R (e.g., range checks, missing data reports, and consistency checks across countries), as well as manual inspection of variables to detect anomalies, coding errors, or inconsistencies. Final datasets will be accompanied by a codebook and documentation detailing all cleaning and transformation steps.

2. Data Documentation and Metadata

2.1 How will you document the data?

The data will be documented with **a comprehensive codebook** containing variable names, labels, response options, coding schemes, and descriptions of derived variables, as well as information on survey design, translation procedures, and sampling methods in each country. Metadata will include details on data collection dates, participating institutions, sample sizes, inclusion/exclusion criteria, and any deviations from the standardized protocol. All metadata and documentation files will be stored in non-proprietary formats (PDF and CSV) alongside the datasets, with version-controlled updates. This documentation will be maintained in a dedicated repository folder to ensure that the data remain fully interpretable to both current collaborators and future researchers.

3. Ethical and legal issues

3.1 How will you manage any ethics and confidentiality issues?

The study will collect survey responses that may include **personal or otherwise confidential information** (e.g., age, gender, country of residence), but no directly identifying information (e.g., name, address, IP address - Qualtrics option is out) is collected as part of the questionnaire. Participants may optionally provide an email address solely for the purpose of being contacted for a possible follow-up study. Email addresses are collected via a separate step, stored separately from questionnaire data within the secure Ghent University environment, and are never shared with research partners or included in analytical datasets. Email addresses are deleted once follow-up recruitment is completed or upon participant request.

All participants will provide informed consent prior to participation, with clear information on the purpose of the study, data usage, storage, and sharing procedures. Data will be **anonymised** (or pseudonymised for those having provided their e-mail address) before analysis, with any indirect identifiers assessed and, if necessary, aggregated or removed to minimise re-identification risk. Pseudonymised datasets are only used for internal aims and won't be shared with others. Only purely anonymised datasets are shared with others.

Confidential datasets will be stored on secure, access-controlled servers at the coordinating institution (Ghent University), with encrypted transfer methods (e.g., SFTP, secure institutional cloud) used for data sharing between collaborators. Access to raw data will be restricted to authorised team members, and all data handling will comply with GDPR and relevant national regulations in participating countries (which is checked by the local collaborators).

3.2 How will you manage intellectual property rights issues?

All primary data collected in the study will be owned jointly by the coordinating institution and participating research partners, in accordance with consortium agreements specifying authorship, usage rights, and responsibilities.

The intellectual property rights (IPR) for the **survey instruments** will remain with their original authors, with permission obtained where required for use and translation. Newly developed items or measures within the project will be made available under a permissive license (e.g., CC BY 4.0) to enable reuse with proper attribution.

Integrated third-party datasets (e.g., Freedom House, World Bank) are openly available and will be used in compliance with their respective licensing conditions, with full citation.

No data sharing will be delayed for the purpose of seeking patents, as the study does not generate patentable outputs. Data intended for public sharing will be anonymised and released under a clear open license, unless contractual or legal obligations require restricted access.

4. Data Storage and Backup during Research

4.1 How will you store and backup data during research?

During the research, all data will be stored on **secure, access-controlled servers provided by the coordinating institution (Ghent University)**, which offer sufficient capacity for the anticipated dataset size. These servers are protected by institutional firewalls and regularly updated security protocols. Data will be **backed up automatically on a daily basis** to encrypted institutional backup servers located in separate physical locations to ensure redundancy. Local copies of working datasets may be stored temporarily on encrypted, password-protected devices of authorised team members, but all master files will remain on the central server. In the event of data loss, recovery will be possible through the institutional backup system, which maintains multiple historical versions of files for a defined retention period, ensuring restoration of the most recent valid version without data corruption.

4.2 How will you ensure that stored data are secure?

Data security risks include unauthorised access, accidental loss, corruption, or interception during transfer. To mitigate these risks, all datasets will be stored on secure, access-controlled institutional servers with encryption at rest and protection by regularly updated firewalls and security software. Access will be restricted to authorised collaborators through individual user accounts with role-based permissions, and accounts will be revoked when no longer required. Collaborators will access data via secure institutional VPN or other encrypted channels to prevent interception. Data transfers between partners will be conducted using encrypted methods such as SFTP, secure institutional cloud services, or password-protected encrypted archives shared through separate communication channels. No data will be transferred via unsecured channels (e.g., unencrypted email attachments), and all team members will follow agreed data handling and security protocols.

5. Data Selection and Preservation after Research

5.1 Which data should be retained for preservation and/or sharing?

An anonymised version of the full international survey dataset will be retained for long-term preservation and potential sharing. This dataset will include all variables necessary to replicate published analyses and to support verification, secondary analyses, and meta-analyses, in line with open science and FAIR principles.

Any identifiable or linkable data, including temporary contact information collected solely for optional longitudinal follow-up, will be deleted as soon as they are no longer required for their intended purpose and in accordance with GDPR and institutional ethics approvals. Such contact data are never included in analytical or shared datasets.

All supporting documentation (such as codebooks, questionnaires, translation and harmonisation records, and analysis scripts) will be preserved alongside the anonymised dataset to ensure transparency, interpretability, and reproducibility of the research.

The anonymised research data and accompanying documentation will be retained for a minimum of 10 years after completion of the project, in accordance with Ghent University policy and funding body requirements. Third-party datasets used in the project (e.g., publicly available country-level indicators) will not be preserved separately but will be referenced with full citations to enable re-access from their original sources.

5.2 What is the long-term preservation plan for the selected datasets?

The anonymised international dataset, along with all accompanying documentation and analysis scripts, will be deposited in a trusted, discipline-appropriate data repository such as the **Open Science Framework (OSF)**. These repositories provide persistent identifiers (DOIs), ensure long-term accessibility, and do not charge deposit fees. Prior to deposit, all files will be curated to meet repository metadata requirements and to ensure clarity for secondary users. In addition, a copy will be retained on the coordinating institution’s secure long-term storage infrastructure, following institutional preservation policies, to provide redundancy and guarantee continued access beyond the end of the research project.

6. Data Sharing

6.1 Are any restrictions on data sharing required?

The datasets will contain personal data at the point of collection, but all shared versions will be fully anonymised to remove direct and indirect identifiers, in line with GDPR and ethical approval requirements. Informed consent procedures explicitly include the possibility of sharing anonymised data for scientific purposes. Third-party datasets (e.g., Freedom House, World Bank) used in the project are openly available and may be shared in derived form, with appropriate citation of their original sources. There is no duty to keep the anonymised dataset confidential beyond these obligations, and no intellectual property restrictions prevent sharing. An embargo period of up to 12 months may be applied to allow for the publication of primary research outputs before public release. Any restrictions on sharing will be mitigated through anonymisation, aggregation, or, if necessary, controlled access via a trusted repository with clearly defined user agreements.

6.2 How will you share data selected for sharing?

The anonymised dataset and accompanying documentation will be made publicly available via a trusted repository such as the Open Science Framework (OSF) within 12 months of primary publication. The data will be shared under a permissive open license (e.g., CC BY 4.0), allowing reuse with proper attribution. Repository deposit will ensure the dataset is assigned a persistent identifier (DOI), enabling citation and acknowledgment in future work. Metadata will include detailed descriptions, keywords, and links to related publications to facilitate discoverability through repository search functions, Google Scholar, and relevant disciplinary databases. In addition, the dataset will be promoted through project publications, conference presentations, and the project website (comugent.be), ensuring that potential users in the academic community can easily locate and access it.

7. Responsibilities and Resources

7.1 Who will be responsible for data management?

The principal investigator, Dr. Joachim Waterschoot, will oversee implementation and periodic revision of the data management plan, ensuring compliance with institutional, funder, and legal requirements. Also, he will be responsible for day-to-day data management activities, including secure storage, version control, quality checks, documentation, and preparation of datasets for sharing. In this collaborative international study, each country lead will be responsible for ensuring data collection follows the agreed protocol. The central team will manage quality checks across countries, integration, cleaning, and archiving of the combined dataset. If the principal investigator leaves the department or university, responsibility for the data will be transferred to an appointed institutional custodian, and the datasets and documentation will remain stored on the institution’s secure infrastructure and in the selected public repository to ensure continuity and long-term accessibility.

7.2 Will you need additional resources to implement your DMP?

Implementation of the data management plan will primarily rely on existing institutional infrastructure, including secure servers, backup systems, and access to trusted repositories, so no major additional hardware or storage costs are anticipated. All anticipated costs for these activities are expected to be covered within the project’s budget.

Data Protection Impact Assessment

1. Does your research fall under the scope of a template DPIA?

- Yes (specify below)

The research falls under the scope of an existing template DPIA for large-scale, multi-country social science surveys involving the collection of special categories of personal data and international data transfers. This template DPIA framework will be used as the basis for assessing privacy risks and documenting the technical and organizational measures taken to protect participants' rights and freedoms.

2. Provide more details for any of the risks that you have ticked in question 25 under the 'GDPR record' tab, so the overall risks related to your processing are clearly and accurately described.

The processing involves several GDPR high-risk criteria.

First, **special categories of personal data** will be collected, including perceptions on political regimes, psychological and mental health, and sexual orientation, which require heightened safeguards to prevent misuse or unauthorised disclosure.

Second, **large-scale processing** will occur, with thousands of participants recruited across multiple countries, increasing both the volume of sensitive data and the potential impact in the event of a breach.

Third, the study will **evaluate aspects concerning health, personal preferences, interests, and behaviour** through validated psychological and well-being measures, which may be considered sensitive in certain cultural or political contexts.

Fourth, **data will be transferred internationally**, including to countries outside the EEA and not on the European Commission's 'white list', which increases the risk of inadequate legal protections unless robust contractual and technical safeguards are in place.

Finally, **datasets will be matched and combined** by linking individual-level survey responses with publicly available country-level indicators (e.g., democracy indices, economic data), which, if not carefully anonymised, could heighten re-identification risk, especially in small samples or rare demographic groups.

3. Explain why the processing of personal data is necessary to achieve the purposes of the research. Include the benefits for individuals and the wider public.

The processing of personal data is necessary to address the central research question of *how perceptions of democracy relate to individual well-being and ill-being across diverse cultural, political, and socio-economic contexts*. To examine these relationships, it is essential to collect information on participants' political attitudes, basic psychological needs, physical and mental health, and socio-demographic characteristics, as these variables allow for rigorous statistical analysis, cross-national comparisons, and the testing of theoretical models. Without personal data, particularly sensitive data on political perceptions and health, it would not be possible to identify the psychological mechanisms linking democratic perceptions to well-being or to detect differences between population groups.

The benefits for individuals and the wider public include a deeper understanding of how democratic systems and experiences can support psychological needs, health, and overall life satisfaction. The findings will inform policymakers, civil society, and international organizations on how to design and implement governance practices that enhance autonomy, inclusion, and social trust, ultimately contributing to healthier, more resilient, and more cohesive societies.

4. Can the processing or part of the processing reasonably be achieved in a different/alternative way, less detrimental to the privacy of data subjects? Evaluate the possible alternatives.

- No

The research objectives require the direct collection of specific personal data, including certain special categories (e.g., political regime perceptions, mental health indicators), to allow for valid testing of the hypothesised relationships between democratic perceptions, psychological needs, and well-being. Using aggregated or fully anonymised public data would not capture the individual-level variables necessary for these analyses, and proxy measures would lack the precision and validity needed to answer the research questions. The study design already minimises privacy risks through strict anonymity of survey data, optional UGent-only pseudonymised re-contact, secure storage, and data minimisation.

5. Describe the steps, measures or controls you are taking to minimise the risk to privacy and safeguard the rights of the persons whose personal data you are collecting.

To minimise privacy risks and safeguard participants' rights, the study will implement both technical and organisational measures throughout the data lifecycle.
Before data collection, participants will be provided with clear, accessible information about the study's purpose, the types of personal data collected, how these data will be processed, and their rights under GDPR, including the right to withdraw at any time.
During data collection, survey data are collected anonymously without assigning participant identifiers. Optional contact data for follow-up are pseudonymised using an internal UGent-only code.
Technical safeguards include encryption of all data at rest and in transit, storage on secure access-controlled institutional servers protected by firewalls, and the use of secure VPN connections for authorised remote access.
Organisational safeguards include granting access only to authorised team members based on role-specific needs, regular review of permissions, and GDPR-compliant data handling training for all researchers involved.
For **paper-based surveys** in countries without reliable internet, physical forms will be stored in locked cabinets, digitised promptly, and securely destroyed after verification.
Data transfers to partners outside the EEA will be conducted via encrypted channels.
After data collection, indirect identifiers will be assessed and, if necessary, aggregated or removed to ensure full anonymisation before analysis and public sharing.
Documentation (e.g., codebooks, protocols) will be maintained to ensure transparency and facilitate ethical re-use of anonymised datasets. These measures collectively ensure the protection of privacy and uphold participants' rights while enabling the research objectives to be achieved.

6. Describe the steps you have taken to make sure the research is as accurate as possible and there are minimal unintended consequences.

To ensure the research is as accurate as possible and to minimise unintended consequences, the study uses **validated and widely used survey instruments** for measuring political perceptions, basic psychological needs, well-being, and health outcomes, ensuring high reliability and validity across cultural contexts. **Questionnaires are translated and back-translated** in each participating country following established linguistic validation procedures to maintain conceptual equivalence. A **harmonised data collection protocol** is used across all sites to guarantee consistency in recruitment, informed consent, and administration procedures.
Data quality is maintained through **real-time monitoring** of online survey responses, automated range and consistency checks, and manual inspection for anomalies or missing data patterns. For paper-based surveys, **double data entry** and verification procedures are implemented to avoid transcription errors.
To avoid unintended consequences, the survey design and questions are reviewed for **cultural sensitivity** and **ethical acceptability**, with potentially sensitive questions clearly marked as optional.
The analysis plan is **pre-registered** to enhance transparency and reduce risks of biased interpretation.
All reporting will present **aggregate, anonymised results** only, avoiding any identification of individuals or small subgroups. Furthermore, findings will be communicated responsibly, avoiding politicised or misleading interpretations that could misrepresent the data or harm public trust.

7. Is the (possible) negative effect or risk for the privacy of the data subjects in reasonable proportion to the processing purposes?

- Yes

The potential privacy risks, such as unauthorised access, re-identification, or misuse of sensitive personal data, are mitigated through robust technical and organisational safeguards, including pseudonymisation, encryption, secure storage, controlled access, and GDPR-compliant international data transfer measures. Given that the research addresses an important scientific and societal question about the relationship between democracy, psychological needs, and well-being, the limited and well-managed risks are in reasonable proportion to the significant potential benefits for individuals and the wider public.

8. How would you describe the likelihood of the risk(s) after having completed the previous questions in this DPIA?

- Limited

While the study involves processing special categories of personal data on a large scale and transferring data internationally, the likelihood of privacy risks materialising is low due to the comprehensive safeguards in place, including pseudonymisation, encryption, strict access control, secure transfer protocols, and full compliance with GDPR. These measures substantially reduce the probability of unauthorised access or re-identification, though the likelihood cannot be considered negligible given the scope and sensitivity of the data.

9. How would you describe the impact of the risk(s) after having completed the previous questions in this DPIA?

- Important

If a privacy breach were to occur, the impact could be significant due to the inclusion of special categories of personal data such as political perceptions, mental health information, and sexual orientation. Such a breach could potentially result in harm to participants, including reputational damage, discrimination, or personal distress, particularly in countries with limited protections for political or sexual minorities. However, the likelihood of such an event is reduced through the extensive technical and organisational safeguards described in this DPIA.

10. How would you describe the risk(s) after having completed the previous questions in this DPIA?

- Acceptable risk(s) left

Although the processing involves sensitive personal data and international transfers, the residual risks after implementing all planned technical and organisational safeguards are minimal and proportionate to the research purposes. These risks are considered acceptable within the framework of GDPR, given the strong data protection measures, clear informed consent procedures, and the significant societal value of the research outcomes.