Research Ethics Appendix Unimi Eco-Social Survey

1. Information on Participant Recruitment:

The Unimi Eco-social cross-national survey involved adult volunteers (18 years old or more) who explicitly agreed to participate in the research only after having been appropriately informed about the purpose of the project, its funding, and organisational and technical measures adopted to safeguard their privacy.

YouGov, the survey company in charge of administering the survey, is amongst the largest and most renowned opinion poll agencies in Europe, considered an expert in conducting cross-national surveys. We made sure that the company was compliant with the GDPR.

The survey was conducted on national samples of voters representative of the adult population in 7 European countries (France, Germany, Poland, Italy, Spain, Sweden, and the UK). National samples were built through a quota-sample design. The main criteria for the sample stratification were age, gender, education and macro-area of residence. More information about the survey is available in the attached methodological note (see attachment 2). The private company that conducted the survey filled the quota of national samples by selecting individuals randomly from their online panels of volunteers. The privacy policy that each panellist voluntarily subscribes to when registering to the panel is available at this link: https://account.yougov.com/gb-en/account/privacy-policy.

2. Informed Consent Procedures:

Given that the survey was conducted online via the CAWI (Computer Assisted Web Interview) method, informed consent procedures were implemented on the online platform provided by the private company selected to conduct the survey, YouGov. A start screen contained the information about the study and the informed consent form, failure to provide consent prevented the participation in the survey. Potential participants selected by the company were firstly informed about the project and, only if they voluntarily agreed to continue, they evaluated whether to give us their informed consent to participate in the survey.

3. Exclusion of Children and Individuals Unable to Consent:

The cross-national survey only involved adult volunteers (18 years old or older). Given the quota-sampling design according to which national samples are stratified by age, gender, education and macro-area of residence, all potential participants who were not 18 years old or older at the moment of recruitment were excluded from the survey. It was ensured that data subjects' personal identity was safeguarded throughout the whole process, from data collection to storage, protection, retention and destruction. The data collected was further processed in a pseudonymised form in accordance with the statistical methodologies that were used for the scientific purpose of the project. More specifically, we adopted pseudonymisation on all information that related to data subjects' personal identity. The collected data was supplied to and received by the project participants only in a pseudonymised form by the private company that ran the survey, YouGov.

4. Measures to Prevent Vulnerability/Stigmatisation:

Although linguistic minorities could be included in the survey, data was anonymised and presented in aggregate form to prevent stigmatisation or vulnerabilities. Necessary technical and organisational measures were employed to ensure confidentiality.

5. Involvement of Vulnerable Participants:

Vulnerable participants were excluded from the research.

6. Data Protection Officer (DPO):

The University of Milan appointed a Data Protection Officer. Contact details:

Dott. Pierluigi Perri

University of Milan

Via Festa del Perdono 7, 20122, Milan, Italy

Email: dpo@unimi.it

7. Justification for Processing Special Categories of Data:

Our research involves "special categories of data" as listed in article 9 of the General Data Protection Regulation 2016/679 insofar it includes citizens' political opinions, in particular attitudes and orientations towards climate change and policies to mitigate it. In compliance with the Art. 9 (paragraph 2.a) of the General Data Protection Regulation 2016/679, justification for the use and processing of these special categories of data are provided by the explicit consent to the processing of those personal data, for the specific purposes of the study, obtained via the Informed Consent Form. The Informed Consent Form is signed by the respondents who agree to participate in our cross-national survey.

8. Technical and Organisational Safeguards:

In compliance with the Art. 32 of the General Data Protection Regulation 2016/679, we implemented all the technical and organisational measures to safeguard confidentiality and, more in general, the rights and freedom of the data subjects during the phases of data collection, storage, protection, retention and destruction. We ensured that the data subjects' identity was protected throughout the whole process, from data collection to storage, protection, retention and destruction. The data collected was further processed in an anonymised or pseudonymised form, aggregately and in accordance with the statistical methodologies used for the scientific purpose of the project. In every research output using public opinion data, the total anonymity of individual data subjects is protected. The collected data is supplied to - and received by - the project participants only in an anonymised form.

The research data is retained in electronic format. The files are and will be stored in a password-protected area of the University of Milan servers (with firewall protection) and never be stored on laptops or elsewhere (e.g. clouds). The data will be kept in an encrypted protected folder that can only be accessed by official members, PIs, Post-Docs and researchers working on the project, and access will be revoked upon termination of the contract.
Anonymised and aggregated data will be made publicly available on internationally recognised institutional or academic data repository. Additional data associated with the project may be destroyed from the servers and locking cabinets upon termination of the project.

9. Anonymisation and Pseudonymisation Techniques:

In compliance with the Art. 32 of the General Data Protection Regulation 2016/679, data collected by the project using a cross-national survey was and will always be stored and processed only in a pseudonymised form, which does not permit the identification of data subjects. In fact, pseudonymised data can no longer be attributed to a specific data subject without the use of additional information. Such additional information will be kept separately and subject to technical and organizational measures to ensure non-attribution to an identified or identifiable individual. More specifically, additional information will be archived solely in one encrypted document on the main server of the university. Pseudonymised data will be stored in a password-protected area of a University of Milan server.

10. Informed Consent and Data Processing:

Participants explicitly agreed that their data would be processed in compliance with GDPR, pseudonymised to separate identifiers from research data, and used only in aggregate, anonymised forms for research outputs. The Attachment 1 document describes the data protection measures that the private company, YouGov, that conducted the survey adopts. Data subjects involved in the cross-national survey voluntarily and explicitly agreed that their personal data would be processed in compliance with the General Data Protection Regulation 206/679. In particular, they agreed that data was to be processed in a pseudonymised form, meaning that the name and other direct identifiers were kept separate from the collected research data so that linkage to identity is not possible outside the authorised members of the research team. Furthermore, data subjects involved in the cross-national survey confirmed also that they know that their data will be used in an aggregate and anonymised form in research outputs only in accordance with the objectives of the project.

11. Ethical Risk Assessment:

Measures to mitigate risks included pseudonymisation, anonymisation, and compliance with ethical codes.

12. Research Findings Misuse Prevention:

Research outputs are peer-reviewed, accompanied by methodological notes, and published in academic journals. Data is publicly disseminated responsibly, with dissemination plans to monitor and address misuse. In conducting their studies all the researchers involved in the project adhere to the ethic codes approved by their institution (University of Milan) and the national and international professional organizations to which they are affiliated (e.g. Italian Association of Political Science -SISP and European Consortium of Political Research - ECPR).
To ensure the correct interpretation of our data, research outputs associated with the project will be published in nationally or internationally recognized academic journals adopting peer-review.
Furthermore, once our data are made publicly available in an internationally recognised institutional or academic data repository, they will be always accompanied by a codebook explaining the type of data and variables included, a methodological note explaining data collection and sampling strategy (see attachment 2), an executive summary with the main findings obtained from our analyses and the explicit request to appropriately quote our studies.
Although we are not fully able to ensure that third parties will not misinterpret and misrepresent the findings of our project, we will make all reasonable efforts to make sure that our research is publicly disseminated outside the academia most appropriately.

13. Profiling:

The research does not involve profiling of participants.

Attachment:

1. Attachment 1 - YouGov data-protection-policy_v6-0.
2. Attachment 2 - Methodological note Unimi_Ecosocial survey.

Group Data Protection

Policy

Scope	Global
Owner of Document:	Group Data Protection Officer
Date of creation:	May 2018
Latest review date:	March 2024
Next review date:	March 2025
Classification	Public
Document code	v6.0

About this policy

As a global data company and provider of research insights we take privacy and data security very seriously and believe that everyone's personal data should be handled responsibly regardless of where an individual lives. Our *Data Privacy Compliance Framework* is therefore based on the principles of the EU's General Data Protection Regulation (GDPR) while also maintaining the flexibility required to ensure we can comply with all other applicable data and security obligations in the markets that we operate.

While our responsibilities may originate from many laws, regulations and guidelines that apply to us, we believe that complying is more than a box-ticking exercise; it is an opportunity to create and reinforce trusted relationships with anyone who provides us with their personal data – from those who participate in our surveys, to our clients and to our employees. It is also an opportunity to enhance our reputation for accuracy and transparency.

This Policy sets out the fundamental data privacy principles by which the YouGov processes personal data. Following the requirements in this Policy will not only ensure compliance with applicable data privacy laws, but it will also allow us to respect the rights of the individuals whose data we hold. If you have an employment contract, service agreement or contract for services with YouGov, you are part of YouGov's workforce, and this Policy applies to you. References to 'employee' in this Policy refer to all members of YouGov's workforce.

Scope

Our Group Data Protection Policy ("Policy") applies to 'research data' processed by all YouGov Group Companies ("YouGov"). Research data is any information collected from individuals that participate in YouGov's research. Non-member participants may be individuals recruited from:

- Client-provided sample;
- Samples that are available to purchase; and
- Public websites or other public sources.

While personal data collected from YouGov's employees and clients are not discussed in this Policy, it is important to note that we process personal data relating to these individuals as a data controller. The applicable privacy notices are available at the following locations:

- Client privacy notice
- Employee privacy notice

The policy

YouGov's role in data processing

This section sets out our role in processing personal data collected from YouGov members and from non-member research participants.

Processing member data

We are a *data controller* (either sole or joint with our clients) when processing personal data collected from our members.

Syndicated research

Syndicated research is survey-based and is created by YouGov, which determines the questions, research methodology, size and scope of the research and samples the members to be invited. The research insights are offered to multiple clients, who purchase subscriptions to the insights (in other words, the research is carried out independently of any one client).

YouGov is the sole data controller of member data when providing syndicated research services because we alone determine the purposes and the means of the personal data being processed.

Custom research

Custom research is survey-based research, conducted for and funded by a specific client (or clients), and the research methodology and resulting insights are tailored to the specific needs of the client. Custom research involves a significant level of collaboration with YouGov's clients.

Because the roles of YouGov and YouGov's clients in data processing for the purpose of custom research vary from project-to-project, based on the tasks carried out by each party, YouGov will be sole data controller for some projects, and for others YouGov and the client will joint data controller. The appropriate processing roles therefore need to be agreed with each client before the research commences.

Processing non-member data

Client sample

When asked to send survey invitations to client-provided sample (for example, our client's customers, employees, or members), we are a *data processor* for the contact information used to send these invitations, the associated survey responses and any identifiable information collected within the survey, for example, contact information used to administer a prize draw.

Purchased & publicly available sample

When we obtain personal data from purchased and publicly available sources, we become the *data controller* for that data as soon as we receive it or upload it to any of our systems. Whenever we obtain personal data from 3rd parties, we perform due diligence to ensure that the data subjects included in the purchased list have been given appropriate notice and, where required, have given their consent. Similarly, we will always consider the privacy implications of obtaining personal data from public websites.

Principles for processing personal data

The data privacy principles adopted by YouGov are established in Article 5 of the GDPR. They outline the basic responsibilities for organisations that handle personal data and are grounded in one of the core themes of the GDPR – that all processing of personal data should be lawful and fair.

Lawfulness, Fairness and Transparency

Personal data must be processed lawfully, fairly and in a transparent manner. This means that our use of personal data needs to be clearly communicated to individuals in an appropriate way and, where applicable data privacy laws require it, each use of personal data must have an underlying legal ground for that processing (discussed further in the following section).

Our research privacy notices (example here) describe the personal data we collect and explain how we use it. These notices are presented to members at appropriate points and, where required, they include a description of the legal grounds that we rely on when processing personal data.

> *What this means for us: we will always give people a choice about participating in our research and be clear with participants about what information is being collected and how it will be used.*

Purpose Limitation

Personal data must be collected for specified, explicit and legitimate purposes and not be further processed in a manner that is incompatible with those purposes. This principle is closely linked to the fairness and transparency principle as personal data can only be used for purposes that individuals have been made aware of.

What this means for us: we will only use the data we have collected for the purposes that we have told people about, and we will always inform and obtain permission (where required) for any further processing outside of those purposes.

Data Minimisation

Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. This means that we should only collect data that is required to enable us to serve our members and deliver our products and services to our clients.

Where possible, anonymisation or pseudonymisation techniques should be applied to personal data to reduce the risks to the individuals concerned. The Data Privacy and Information Security teams can help in putting these techniques in place.

What this means for us: we will only collect the information that we need to provide our research and data analytics services, which aligns with the goals of our researchers to minimise the number of questions asked.

Accuracy

Personal data must be accurate and, where necessary, kept up to date. Reasonable steps must be taken to ensure that personal data that are inaccurate are erased or rectified in a timely manner.

What this means for us: we will continuously update the data we use to ensure that the data used in providing our services are accurate so our clients can rely on robust insights.

Storage Limitation

Personal data must be kept for no longer than is necessary for the purposes for which the data are processed. This means that when collecting personal data, we must be clear on the period that the data is needed for, and if necessary, identify different retention periods for different types of data. For example, video recordings that are collected as part of a qualitative study may not need to be kept for as long as the resulting transcripts. While data retention periods should be reasonable for each processing activity, data should not be kept 'just in case'.

What this means for us: we will inform participants, via our privacy notices, of the considerations involved in determining the time we store their data, and not store any data for longer than is needed to provide our services.

Integrity and confidentiality

Considering the state of technology and other available security measures, the implementation cost, and the likelihood and severity of personal data risks, appropriate technical or organisational measures must be used to process personal data in a manner that ensures the security of personal data. This includes protection against accidental or unlawful destruction, loss, alternation, unauthorised access to, or disclosure. This principle, focusing on the handling and storage of data, is particularly important in protecting our reputation and the trust of those who provide data to us.

What this means for us: we use appropriate security measures to protect the personal data that we hold to reduce the risk of personal data breaches and to build confidence in us.

Accountability

The GDPR introduced the accountability principle to oblige organisations to prove their compliance. This means we are responsible for demonstrating compliance with the principles outlined in this section. Accountability can be demonstrated in several ways, including creating data processing inventories, internal policies and guidelines and completing data protection impact assessments.

What this means for us: we document our approach to data privacy to demonstrate our compliance to applicable data privacy laws. This helps to build trust with everyone who interacts with us.

Fair processing

While fair processing (or privacy) notices are not specific to the GDPR, the GDPR makes it clear that personal data can only be processed when a clear description of the collection and use of that data is communicated to individuals. This is done via our privacy notices, which give individuals all the information they need about how we collect and use personal data. Our research privacy notices are specific to the markets and languages we operate in.

If a use of personal data is not included in our privacy notices, then we cannot use personal data in that way until our notices are updated and, if required, the changes are communicated to individuals. YouGov's privacy framework requires that any new collection or use of personal data is assessed by the Data Privacy team (see the 'Privacy by design'' section for more information).

This section outlines the legal grounds for processing that we rely on to collect and use personal data (where a legal ground needs to be established under the applicable privacy laws).

Legal grounds for processing

While the concept of 'legal grounds' is not limited to the GDPR, YouGov looks to apply the principles of the GDPR globally where possible. Article 6 provides six legal grounds for processing personal data. Where the GDPR applies, each use of personal data must be based on one of these grounds for that use to be lawful. We rely on three legal grounds for processing member personal data:

1. Processing being necessary for the legitimate interest of a data controller;
2. Consent; and
3. Processing is necessary for the performance of a contract.

These grounds for processing are communicated in our privacy notices and are discussed below.

Relying on 'legitimate interests'

When relying on legitimate interests, a business must balance its own interests against the interests, rights, and freedoms of individuals. We rely on 'legitimate interests' to process most of the personal data collected in providing our market research services because we use data in ways that individuals would reasonably expect, and which have a minimal privacy impact.

Because fair processing notice is key to relying on legitimate interests, individuals are given the following information in our privacy notices (which are available in languages that are appropriate for the markets we operate in):

- The identity and contact details of the data controller
- The types of personal data collected, and how it is used
- How long personal data is stored
- The types of organisations that personal data are shared with
- The security measures used to protect personal data
- Safeguards that are in place for potential international data transfers
- The rights that individuals have with respect to their personal data, including how to lodge a complaint

In relying on legitimate interests, we acknowledge that we must be careful to consider and protect people's rights and interests.

Relying on consent

YouGov relies on consent in the following circumstances:

1. Processing special category data (otherwise known as 'sensitive personal data'). Depending on which country a participant is from, members will either be asked to consent to our use of different categories of sensitive personal data when they join YouGov (which can be withdrawn in their account page), or they will give a more general consent when they join. The

method of obtaining consent from those included in a client-provided sample will ultimately be decided by our client (as the data controller).
2. Sharing personal data with our clients: depending on the client's intended use of the data, the consent mechanism is included within the survey and respondents can choose whether or not they want to provide this information.
3. Carrying out specific data processing activities where we have determined that consent is the most appropriate ground, for example, YouGov Safe.

Where we are required to, we apply the GDPR's standard for consent: it must be a freely given, specific, informed, and unambiguous indication of a person's wishes, involve a clear affirmative action (an opt-in) and give granular consent options for distinct processing operations.

Relying on 'necessary for the performance of a contract'

YouGov relies on processing being necessary for the performance of a contract when collecting and using 'user data' via YouGov Finance, which is the information obtained from YouGov member's bank transactions. Note also that personal data processing via YouGov Finance also relies on legitimate interest (for silent / third party data included within user bank transactions) and consent (for special category data included within user bank transactions).

Third parties and international transfers

Sharing data within the YouGov Group

YouGov is a global organisation, so some of the personal data that we collect may be transferred within the YouGov Group of companies to enable us to provide our services. For example, a client may want to run a survey in multiple countries, or we may need our operations teams in Romania or India to provide data processing services.

To ensure these transfers are secure, all YouGov Group companies have entered into an Intra-Group Sharing Agreement that provides contractual safeguards in relation to personal data shared between group companies. This Agreement utilises approved Standard Contractual Contracts to address any data that is being transferred out of the European Economic Area ("EEA").

Sharing data with third parties

Data processors

Any third parties used to process personal data on our behalf are 'data processors', or 'service providers'. Service providers are assessed within the Governance Team's *Supplier Approval Process*, which includes appropriate data privacy, data security and compliance due diligence.

Data controllers

Where YouGov shares data with, or receives data from, another organisation where each party is using that data for its own purposes, this will constitute data sharing between two data controllers. In these cases, the sharing must be based on one of the six grounds for processing personal data, and an appropriate data sharing arrangement must be agreed by the parties.

Cross-border transfer of personal data

While all reasonable steps are taken to ensure that personal data remains within the country or region where it originated, in some cases we need to share data with other YouGov Group Companies (as noted above) or third parties that are in other countries. In these cases, adequate safeguards are put in place to make sure personal data remains adequately protected. These safeguards may include Standard Contractual Clauses, adequacy decisions or certifications.

'Privacy by design' and 'Privacy by default'

We have adopted a 'privacy by design' approach to ensure that data privacy and security considerations are built into all business activities that involve personal data. Privacy by design promotes data privacy compliance by ensuring that data privacy is a key consideration in the early

stages of any project, and then throughout its lifecycle. We also, by default, only process personal data which are necessary for the specific purposes we are trying to achieve, and never collect excessive amounts of data. We also limit periods of storage and control access to personal data.

YouGov's privacy by design approach

A privacy by design approach helps to identify and minimise risks in using personal data. YouGov's framework has been designed to ensure that:

1. We draw on internal and external expertise to assess new uses of personal data against its responsibilities under appropriate data privacy laws;
2. Uses of personal data across the business are communicated to and understood by all employees; and
3. Users of personal data are aware of their responsibilities in handling personal data.

DPIAs, LIAs and the Privacy Executive Committee

Central to our approach is the use of Data Protection Impact Assessments (DPIA) to identify and mitigate against any data privacy risks arising from activities where the processing of personal data may result in a high risk to individuals. We can use DPIAs to help us make informed decisions about the acceptability of data privacy risks, and to demonstrate compliance with our responsibilities under applicable data privacy laws. We also use Legitimate Interest Assessments (LIA) to determine if 'legitimate interests' can be relied on as a valid legal ground for processing.

In addition, YouGov's Privacy Executive Committee (PEC) has been established to consider new uses of personal data that are brought forward by the Group Data Protection Officer, and whose approval is required based on the level of risk they present.

Training and awareness

All YouGov employees are required to attend and / or complete any training and awareness initiatives that may be assigned.

Online training modules

We use online training modules to deliver training on data privacy and security topics. These modules, and any refresher modules assigned, are mandatory for all YouGov employees globally. Further information is provided in YouGov's Group Mandatory Training Policy.

Other training sessions

Employees may also be required to attend in-person training sessions. Attendance will be determined on a case-by-case basis, depending on the topic and/or the audience.

Data Subject Rights

Data privacy laws set out the rights that individuals have in relation to the data they provide to organisations. These rights are designed to give individuals more control over their data, and organisations must inform individuals about the rights that are available to them and respond within specific timeframes.

The rights that are available to our data subjects are explained in our privacy notices, and our internal guidelines that outline the procedures used to authenticate and respond to all requests.

Right of access

Individuals have the right to know whether an organisation is processing personal data about him or her, and where that is the case, the organisation must provide access to the personal data. This is an absolute right, meaning that it is available regardless of the legal grounds for processing relied on.

Right to rectification

Data subjects have the right to request that a data controller rectifies inaccurate personal data about him or her, and to request the controller to rectify incomplete personal data (taking into account the purpose of the processing).

Right to erasure

Individuals have the right to have their personal data erased and no longer processed. On receiving a valid request to delete an individual's data under the right to erasure, we will identify and permanently remove from our systems all directly identifiable data that is held about that individual, so any data remaining after erasure will have been rendered anonymous.

Right to restriction

Data subjects have the right to request that a data controller restrict the processing of his or her personal data in certain specific circumstances.

Right to data portability

Data Subjects may have the right to receive, upon request, a copy of the data they provided to us in a structured format and to transmit those data to another controller. The right to data portability is not available when relying on 'legitimate interests', so where YouGov relies on 'legitimate interests', the right of data portability is not available to YouGov's data subjects.

Right to object

Data subjects have the right to object to certain types of processing of their personal data in certain specific circumstances.

Responding to personal data breach incidents

When we learn of a suspected or actual personal data breach, the Data Breach Response Team will perform an internal investigation and take appropriate remedial measures in a timely manner, according to the YouGov's Personal Data Breach Policy.

Our Personal Data Breach Policy outlines the procedures that must be followed to ensure that personal data breaches are:

1. Identified and reported to the Group Data Protection Officer
2. Assessed to determine the likelihood and level of risk resulting from the breach
3. Reported, if necessary, to supervisory authorities or communicated to affected individuals
4. Recorded to ensure a clear audit trail of events and decisions

The Personal Data Breach Policy also sets out the roles and responsibilities of the YouGov employees who are involved in the procedures and, if required, notification of a data breach.

Organisation and responsibilities

The responsibility for ensuring appropriate processing of personal data lies with everyone who works for or with YouGov. The following organisational roles have important responsibilities with regards to the processing of personal data:

YouGov Board of Directors

YouGov's Board makes decisions about and approves our general strategies on data privacy and data security matters. The Board endorsed YouGov's GDPR compliance programme and receives a data privacy and security update at each board meeting.

Privacy Executive Committee (PEC)

An effective privacy framework includes a governing body, a defined set of procedures and a plan to execute those procedures. YouGov's governing body is the PEC, which exists to consider new uses

of personal data for approval based on the high level of privacy risk they present. PEC also fulfils the requirement that the Group Data Protection Officer has a direct reporting line into the YouGov Board.

Group Data Protection Officer (DPO)

The Group DPO is charged with monitoring compliance with data privacy regulations and should be involved in all issues relating to the use of personal data. The DPO's primary concern is enabling compliance with all applicable data privacy laws and fostering a data privacy culture within YouGov. The minimum responsibilities of the DPO vary, but per Article 39 of the GDPR they are:

- Monitoring compliance with the GDPR;
- Providing advice in relation to a data protection impact assessments; and
- Cooperating with the supervisory authority and acting as the contact point.

Chief Governance & Compliance Officer

The Chief Governance & Compliance Officer is responsible for driving the strategic direction of YouGov's governance efforts generally. As the Chief Governance & Compliance Officer's remit includes YouGov's group data privacy and legal functions, this role is key in ensuring that data privacy and legal resources come together.

Global Head of IT & Group Head of Information Security

These two employees are responsible for:

- Ensuring that all systems, services and equipment used for storing data meet acceptable security standards;
- Performing regular checks and scans to ensure hardware and software is functioning properly, securely configured and free of vulnerabilities that could impact the security of personal data; and
- Improving suppliers' awareness levels of personal data privacy and ensuring data privacy responsibilities are passed on to suppliers that process personal data for YouGov
- Auditing the security of third parties, where appropriate and possible.

Conflicts of law

This Policy is intended to comply with the laws and regulations in the place of establishment and of the countries in which YouGov operates. In the event of any conflict between this Policy and applicable laws and regulations, the latter shall prevail.

Scope, Monitoring and Review, Version Control

Scope

This policy covers all global employees, officers, consultants, contractors, freelancers, interns, work experience students, casual workers and agency workers (collectively referred to in this policy as "staff") of YouGov plc and subsidiary companies. This policy does not form part of any employee's contract of employment and we may amend it at any time.

Monitoring and Review

The Group Data Protection Officer will review the implementation of this policy in respect of its suitability, adequacy and effectiveness and make improvements as appropriate.

Version Control

Version	Name	Date	Changes
v1.0	EU Data Protection Policy	15 May 2018	• First version
v1.1	EU Data Protection Policy	21 May 2018	• Minor amends
v2.0	EU Data Protection Policy	28 Nov 2018	• Changed document classification to 'Public' • Updated definition of 'employee' • Added new section for 'Training & awareness'
v.3.0	Global Data Protection Policy	15 Mar 2019	• Updated to expand the Policy scope from EU to Global
v3.1	Group Data Protection Policy	23 Mar 2020	• Changed policy name to 'Group Data Protection Policy' • Updated 'About this policy' to mirror our Data Commitment on YouGov's corporate site • Removed 'Definitions' section • Minor text changes
v4.0	Group Data Protection Policy	11 Mar 2021	• Replaced references to 'panellists' with 'members' to reflect updated business terminology. • Removed references to 'data governance' to avoid confusion with the Data Governance team. • Added LIAs in the *Privacy by Design* section.
V5.0	Group Data Protection Policy	28 Mar 2022	• Changed some references of 'Data Protection' to 'Data Privacy' to align with internal re-brand of the Data Privacy team. • Added additional YouGov-specific information in the 'Principles of processing personal data' section. • Added additional detail on 'legitimate interests' and 'consent'. • Added a section on 'Privacy by Default'. • Removed reference to the role of the Global Panel Director.
v5.1	Group Data Protection Policy	23 Sept 2022	• Changed the reference to *YouGov's Data Protection & Security Training Policy* to *YouGov's Group Mandatory Training Policy*.
v5.2	Group Data Protection Policy	24 March 2023	• Included information about YouGov's use of 'performance of a contract' for YouGov Finance. • Minor text amends for clarity and grammar.
v6.0	Group Data Protection Policy	28 March 2024	• Fixing minor typos. • Updated the 'About this policy' section. • Updated the 'YouGov's role in data processing' section to reflect changes to our position paper on that topic.

Eco-social project – Methodological note

- YouGov conducted a survey for the Department of Social and Political Sciences of the University of Milan, as part of the project 'Departments of excellence 2018-2022', intending to develop a database with the purpose of collecting opinions of European citizens on topical issues such as climate change, transition to 'a green economy', and consequent recalibration of welfare systems. The project will be hence named 'Eco-social' in this document.

- The Eco-Social project was conducted in 7 countries (Germany, France, Italy, Spain, Sweden, Poland, and the UK) via CAWI methodology (computer-assisted web interviews), using YouGov's proprietary panel in all countries. The survey is GDPR-compliant.

- Interviews were conducted between December 1th and 9th.

- The number of complete interviews was around 1,500 per country, representative of each country's population in terms of: (i) age bands; (ii) gender; (iii) NUTS1 regions; (iv) ISCED educational levels:
    - The representativeness was obtained using a quota sample design (based on the aforementioned variables) and the relative weight scheme after data collection in order to fine-tune the social-demographic balance of the sample;
    - Thus, the delivery of the dataset includes a "weight" variable that we recommend using in order to adjust quotas representativeness in each country.
- Selected respondents (those sampled according to the quota sample design) received an email inviting them to complete the survey that could be answered via computer, tablet or smartphones. After starting it, they were allowed to restart from the point they stopped at any moment.

- In questions concerning trade union membership, party affiliation or political ideology, respondents were given the chance of not providing an answer.
- A conjoint experiment was implemented in the questionnaire script and repeated twice for each respondent, wherein two policy proposals were compared (Policy A or Policy B); each proposal was composed of three Factors (1, 2 and 3); each factor allowed for one among 3 or 4 levels (A, B, C for Factor 1, A, B, C, D for Factors 2 and 3) to be displayed; some of these levels from different factors could not be displayed in combination for the same proposal at the same time, in order to ensure logical consistency for the respondent.

Weight report and total numerosity per country:

Country	Germany	France	Italy	Spain	Sweden	Poland	UK
Total Complete Respondents (after quality-cleaning)	1510	1564	1524	1527	1539	1528	1,776
Weighting efficiency	99.6	99.2	99.8	99.7	99.4	99.9	95.3
Mean weight factor	1	1	1	1	1	1	1
Minimum weight factor	0.81	0.85	0.93	0.88	0.88	0.94	0.75
Maximum weight factor	1.23	1.34	1.08	1.12	1.30	1.13	2.93
Weight factor ratio	1.51	1.58	1.17	1.26	1.48	1.20	3.89

Please us the Excel file *Edu_quotas_UNIMI_Eco-Social_client* to view the quota scheme used for sampling and weighting.

Fieldwork info:

COUNTRY	fieldwork period		statuses				Length of interview
	first started	last ended	completes before cleaning	starts	incomplete	quota full	median
UK	01/12/2022	09/12/2022	1,777	2,008	229	NA	00:20:43
France	01/12/2022	09/12/2022	1,576	1,747	170	NA	00:20:22
Germany	01/12/2020	06/12/2022	1,525	1,608	83	NA	00:19:53
Italy	01/12/2020	06/12/2022	1,531	1,694	157	NA	00:19:36
Spain	01/12/2020	06/12/2022	1,534	1,739	203	NA	00:19:38
Sweden	01/12/2020	09/12/2022	1,542	1,738	196	NA	00:19:15
Poland	01/12/2020	06/12/2022	1,535	1,756	218	NA	00:19:07

Additional information about YouGov panel:

Recruiting method

We recruit through a mixture of channels, deliberately in order to ensure that we reach the broadest possible audience.

If a panellist responds to a survey invitation from YouGov we will find them a points-earning survey to take even if the original study to which they were invited has closed. This *helps to prevent over-claiming, because a panellist does not feel pressure to qualify for any particular study or else risk losing out on points*.

Sampling method

Our sampling algorithm continuously assesses a random portion of panellists eligible to receive an invitation against the project's demographic requirements time. Each panellist in the random portion who is eligible for a live project will receive an invitation by email. As a reward for completing surveys, panellists earn points that they can convert into gift cards.

Quality assurance

We take a few steps within a user's first interactions with us to ensure that YouGov panellists are human and maintain only one account. These checks are deployed globally and consistently. At the point of attempted registration, we use Captcha technology and assess automatically various aspects of the user's profile and journey to that point: we block accounts associated with blacklisted email domains and we monitor referral traffic to ensure that each new account is unique. We have developed a machine learning application which constantly scans relationships between accounts to help us determine whether an individual user has attempted to create more than one account.

Third party panels management

We only work with globally recognised providers and run a preferred provider scheme. Before qualifying as a 'global preferred provider' a partner must pass our data quality checks (wherein we benchmark their

respondents with our own and external data), provide acceptable answers to the “Esomar 28” standard questions.

For further info on our approach to panel management, according the ESOMAR 28 questions, please read the following document http://cdn.yougov.com/cumulus_uploads/document/t3r5k565j5/ESOMAR_28.pdf