Privacy and Data Protection

Global Privacy and Data Protection Policy

This policy is provided to show Ipsos' internal responsibilities to demonstrate our commitment.

It is neither this website's privacy policy nor suitable or intended for any surveys undertaken by Ipsos and does not create any obligations towards third parties.

Internal links have been removed

Table of contents

1. Introduction

As part of its social responsibility, Ipsos is committed to international compliance with data protection laws, regulation and rules. This privacy & data protection policy ("**Policy**" or "**Data Protection Policy**") applies worldwide to the Ipsos Group and is based on globally accepted basic principles on data protection. This Policy adopts the fundamental principles of the EU's General Data Protection Regulation ("**GDPR**") as the minimum standard to which Ipsos Group, its employees and suppliers must adhere. Although this should go without saying, it does not make the GDPR itself applicable to Ipsos Group globally.

Ipsos depends on the collection and analysis of information about identifiable living individuals ("**Data Subjects**") to carry out its market research and associated business. Maintaining respondents' and the public's confidence requires that respondents do not suffer direct adverse consequences, risk or harm as a result of providing Ipsos with their information or their Personal Data (for a definition and explanation of this term and other capitalised terms, please see the Glossary at the end of this document) being processed for Ipsos's business purposes. The information may be obtained from any kind of individual or organisation.

To conduct its business, Ipsos also needs to collect and process certain types of information, including Personal Data, about people with whom Ipsos deals. These include current, past and prospective employees, suppliers, clients and others with whom it might communicate. In addition, Ipsos may occasionally be required by law to process certain types of Personal Data to comply with certain legal requirements.

This Policy describes the minimum standards of how Personal Data must be processed, collected, handled and stored to meet Ipsos's data protection standards.

Data Users are obliged to comply with this Policy when processing Personal Data on Ipsos's behalf. Any breach of this Policy may result in disciplinary action, up to and including dismissal from Ipsos.

2. Scope

The Policy is applicable globally to all Ipsos companies, regardless of where they are based. Within Ipsos, this Policy will form the minimum standard to which all Ipsos companies, employees and suppliers must adhere, regardless of whether GDPR directly applies to any specific activity or territory.

Everyone who works for Ipsos has some responsibility for ensuring Personal Data are collected, stored and handled appropriately.

It is everyone's responsibility that Personal Data are handled and processed in line with this Policy and its data protection principles.

Ipsos also expects that its suppliers/vendors comply with the principles as set out herein.

3. Application of National Laws and Codes of Conduct

This Data Protection Policy adopts the internationally accepted privacy principles as enhanced by the GDPR. It is subsidiary to and supplements any applicable national legislation. The relevant national laws will take precedence if there is a conflict with this Policy or it has stricter requirements than this Policy. Any registration, notification or reporting requirement for data processing under national laws must also be observed. The contents of this Policy must also be

observed in the absence of corresponding national legislation or where national legislation has a lower standard.

Each company of the Ipsos Group is responsible for compliance with this Data Protection Policy and applicable legal obligations. If there is reason to believe that legal obligations contradict the duties under this Data Protection Policy, the relevant Company must inform the country DPO and the Global Chief Privacy Officer. In the event of conflict between national legislation and the Data Protection Policy, Ipsos will work with the relevant company to find a practical solution that meets the requirements and satisfied the purposes of this Policy as well as applicable legislation.

In addition to this Policy, for its market research business Ipsos adheres to the requirements of the ICC/Esomar International Code on Market, Opinion and Social Research and Data Analytics, which can be found here.

4. Principles for Processing Personal Data

All Personal Data must be dealt with properly, irrespective of how they are collected, recorded and processed - whether on paper, in a computer file, database, or recorded on other material - and there are generally accepted principles to safeguard this, as set out in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, as well as relevant safeguards in various statutes across the world, including the GDPR.

Ipsos regards the lawful and correct treatment of Personal Data and maintaining the confidence of those with whom it deals in Ipsos's appropriate dealing with Personal Data as a vital component of its business operations and is committed to act ethically and responsibly in respect of these Personal Data and always to provide a high degree of confidentiality and security.

To demonstrate these commitments, Ipsos adheres to the principles relating to the processing of Personal Data found in the GDPR which are themselves an embodiment of the OECD principles. Ipsos respects the following principles, which are explained in more detail later, concerning Personal Data. Personal Data will be:

- Processed fairly and lawfully.
- Processed for limited purposes and in an appropriate way.
- Adequate, relevant and not excessive for the purpose.
- Accurate.
- Not kept longer than necessary for the purpose.
- Processed in line with Data Subjects' rights.
- Secure.
- Not transferred to people or organisations situated in other countries without adequate protection.

4.1. Lawfulness, Fairness and Transparency

Personal Data must be processed and collected lawfully, fairly and in a transparent manner in relation to the Data Subject. Furthermore, Data Subjects must be informed of how his/her data are being handled, usually in the form of a privacy policy or terms and conditions. In general, Personal Data must be collected directly from the individual concerned. Where this is not the case the legal basis on which the processing is nevertheless justified must be documented. The relevant DPO has to be consulted on whether a Data Protection Impact Assessment (DPIA) must be conducted (see also the separate guidance on DPIAs that can be found on the intranet).

4.2. Purpose Limitation

Personal Data must only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Subsequent changes to the purpose are only allowed to a limited extent and require substantiation and validation. The relevant DPO has to be consulted on whether a DPIA must be conducted (see also the separate guidance on DPIAs that can be found on the intranet).

4.3. Data Minimisation

Personal Data must be adequate, relevant and limited what is necessary in relation for the purpose for which they are processed. It must be determined whether and to what extent the collection and processing of Personal Data is necessary to achieve the purpose for which the processing is undertaken. Where the purpose allows and where the expense involved is in proportion to the risks to Data Subjects, anonymized data must be used instead of Personal Data.

4.4. Accuracy

Personal Data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard for the purpose for which they are processed, are erased or rectified without delay.

4.5. Storage Limitation

Personal Data must not be retained in a form which permits identification of Data Subjects for longer than is necessary for the purpose for which the Personal Data are processed. Ipsos will not keep Personal Data longer than is necessary for the purpose or purposes for which they were collected. Ipsos will take all reasonable steps to destroy, or erase from its systems, all Personal Data which are no longer required. This does not apply to anonymised data.

Whilst Ipsos Group has introduced policies in line with ISO 20252 about the maximum retention periods for Personal Data, it is also Ipsos's policy to reduce such retention periods whenever possible, either by deleting or anonymising the relevant Personal Data.

4.6. Integrity and Confidentiality

Personal Data must be processed in a manner that ensures appropriate security of the Personal Data from being revealed, disseminated, accessed or manipulated. Therefore, where methodologically possible and the expense is not disproportionate to the Data Subject's risks, Personal Data must be pseudonymised as soon as possible and be used for no other further processing – REMINDER: pseudonymised data remain and are Personal Data!

Once the purpose of the processing has been achieved, usually once quality control has been completed, the Personal Data must be anonymised.

4.7. Restriction on Transfers

Personal Data must not be transferred to other countries (even to other Ipsos companies in other countries) that do not offer an adequate level of protection. Ipsos has introduced various measures to adduce such adequate level of protection on a general basis (see also paragraph 6 for more detail), however, various countries may have stricter, further and/or different requirements that must be adhered to.

4.8. General Measures and Considerations

Additionally, in respect of its market research business Ipsos complies with the ICC/ESOMAR International Code on Market, Opinion, and Social Research and Data Analytics and Esomar's Data Protection Checklist.

5. Legal Grounds for Data Processing

Ipsos will be collecting, processing and using Personal Data only under the following legal bases, always provided that such legal basis exists under applicable national law. One of these legal bases is also required if the purpose of collecting, processing and using the Personal Data is to be changed from the original purpose, unless there is clear compatibility between the original purpose and the new purpose. See also paragraph 4.2 and any potential additional compliance requirements.

5.1. Respondent Data

Respondents are the most common Data Subjects in Ipsos's business. Consequently, the correct treatment of their Personal Data is at the heart of Ipsos's business.

5.1.1 Consent to Data Processing

Personal Data can be processed following consent by the Data Subject. Before giving consent, the Data Subject must be informed in accordance with the transparency principle as set out under paragraph 4.1. The declaration of consent must be obtained in writing or electronically for the purposes of documentation. In some circumstances, such as telephone surveys, consent can be given verbally. In all cases, the granting of consent must be documented.

Any consent will only be valid if it constitutes a freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which it gives a statement, by a clear affirmative action signifying agreement to the processing of the Personal Data relating to him/her. For guidance in respect of consent, please see the intranet.

5.1.2 Data Processing for a Contractual Relationship

Apart from consent, Personal Data may be processed where this is necessary in the context of a contract with such Data Subjects to fulfil the contracts relevant obligations and rights. This applies also where such processing in necessary in order to establish or terminate a contract. This applies in particular to respondents (including mystery shoppers) in the sign up to the Ipsos panels.

Some countries see the entering into a contract as a form of consent.

5.1.3 Data Processing Pursuant to Legal Authorisation

The processing of Personal Data is also permitted if legislation requests, requires or allows this. The type and extent of data processing must be necessary for the legally authorised data processing activity and must comply with the relevant legal provisions.

5.1.4 Data Processing Pursuant to Legitimate Interest

Personal Data may also be processed, if it is necessary for the legitimate interests of the Ipsos Group and where national legislation provides for this basis (e.g. GDPR Article 6(1)(f)). The legal basis of legitimate interest for processing is not recognised in every country, and relevant national legislation will take precedence. Generally, Personal Data of children may not be processed based on legitimate interest and it does not apply to special categories of Personal Data!

In any event, Personal Data may not be processed on the basis of a legitimate interest if, in the individual case, there is evidence that the interests of the Data Subject merit protection and that this protection takes precedence. Before Personal Data are processed on the legitimate

interest basis, it is necessary to undertake a legitimate interest assessment (in the form of a DPIA with a particular focus on the legitimate interest).

5.1.5 Processing of Special Categories of Personal Data

Special categories of Personal Data can be processed only if the law requires this or the Data Subject has given his/her explicit consent. For guidance in respect of consent and particularly 'explicit consent', please see the intranet. Special categories of Personal Data can also be processed if this is mandatory for asserting, exercising or defending legal claims. Within the European Economic Area (EEA), special categories of Personal Data may also be processed for scientific and historical research and for statistical purposes (Article 9(2)(j) GDPR), subject to appropriate additional measures. Before relying on this provisions, a DPIA must be conducted (see also the separate guidance on DPIAs that can be found on the intranet.

5.1.6 User Data and Internet

If Personal Data are collected, processed and used on websites or in apps, the Data Subject must be informed of this in a privacy statement including, if applicable, information about cookies or similar technical measures. The privacy statement and any cookie information must be integrated so that it is easily identified, directly accessible, easily understandable and consistently available by and for the Data Subject.

If use profiles (tracking) are created to evaluate the use of websites and apps, the Data Subjects must always be informed accordingly in the privacy statement. Tracking of Data Subjects online may only be effected, if it is permitted under national law or upon consent of the Data Subjects. Even if tracking uses a pseudonym for the Data Subject, is conducted using cookies, beacons, tags, pixels or any other tracking technique, as a minimum the Data Subject should be given the chance to opt out in the privacy statement. Special care needs to be taken within the EEA to adhere to the ePrivacy Directive and in due course the ePrivacy Regulation.

If websites or apps can access Personal Data in an area restricted to registered users/respondents, the identification and authentication of the Data Subject must offer sufficient protection during access.

As part of Ipsos's commitment to adhere to the Esomar Code, the rules and requirements set out in Esomar's other guidelines like Online Research Guideline and Guideline on Research and Data Analytics with Children, Young People, and Other Vulnerable Individuals also apply to Ipsos as part of this Policy. Also to be considered is the additional guidance published by Esomar as part of its web-based complaints process at www.trustinresearch.org.

5.2. Personal Data Provided by Clients

Transmission of Personal Data to Ipsos by its clients is a common occurrence. It usually happens to provide us with sample or to enhance existing sample. In respect of any Personal Data so received, Ipsos will be the Processor and may only Process these Personal Data in accordance with the instructions agreed with or received from the client. These instructions may include restrictions on transfers to other parties (including other Ipsos companies or suppliers) or transfers to other countries as well as specific security requirements. Any such restrictions must be complied with. It is imperative that such instructions are documented in writing and agreed before any relevant contractual arrangements are accepted by Ipsos, to ensure that Ipsos is actually able to comply with any such client specific restrictions or requirements.

Irrespective of any client requirements, any Personal Data provided by a client may only be:

a) Processed for the purpose they were provided for;
b) Not be kept for longer than is required for the purpose; and
c) Subject to the same security requirements applicable to Ipsos's own Personal Data.

5.3. Employee Data

5.3.1 Data Processing for the Employment Relationship

In employment relationships, Personal Data can be processed if needed to initiate, carry out and terminate the employment agreement. When initiating or considering an employment relationship, the applicant's Personal Data can be processed. If the candidate is rejected his/her data must be deleted in observance with the required retention period unless the applicant has agreed (such agreement to be documented) to remain on file for a future selection process. Consent is also needed to use the data for further application processes before sharing the application with other Ipsos Group companies.

In an existing employment relationship, data processing must always relate to the purpose of the employment agreement if none of the following circumstances for authorised data-processing apply.

If it should be necessary during the application procedure to collect information on an applicant from a third party, the requirements of the corresponding national laws must be observed. In cases of doubt, consent must be obtained from the Data Subjects.

There must be legal authorisation to process Personal Data that is related to the employment relationship but was not originally part of performance of the employment agreement. This can include legal requirements, collective regulations with employee representatives, consent of the employee or the legitimate interest of the company.

5.3.2 Data Processing Pursuant to Legal Authorisation

Please see above at paragraph 5.1.3 for the further requirements. This typically relates to tax reporting or other statutory reporting requirements.

5.3.3 Collective Agreements on Data Processing

If a data processing activity exceeds the purposes for fulfilling a contract, it may be permissible if authorised through a collective agreement between the employer and employee representatives, within the scope allowed under the relevant employment law. The agreements must cover the specific purpose of the intended further data-processing activity and must be drawn up within the parameters of national data protection and employment legislation.

5.3.4 Consent to Data Processing

Employee data can be processed upon consent of the person concerned. Declarations of consent must be submitted voluntarily. Within the EU/European Economic Area, consent generally does not constitute a valid legal basis for the processing in the employment context as there is a legal presumption that such consent was not submitted voluntarily and any processing will have to rely on one of the other legal bases available. Involuntary consent is void. To the extent that consent is a valid basis for processing, please see above at paragraph 1 for the further requirements. In any event consent can normally be withdrawn, thereby preventing any further processing, making another legal basis preferable in any event.

5.3.5 Data Processing Pursuant to Legitimate Interest

Personal Data may also be processed if it is necessary to enforce a legitimate interest of the Ipsos Group, provided the applicable law allows for the processing of Personal Data based on a legitimate interest. Within the employment context, legitimate interests are generally of a legal or financial nature.

Please see above at paragraph 5.1.4 for the further requirements and limitations for the application of legitimate interest.

Monitoring, control or supervisory measures that require processing of employee data may only be taken if there is a legal obligation to do so or there is a legitimate reason. Even if there is a legitimate reason, the proportionality of the control measures must also be assessed before such measures are applied. The justified interests of the company in applying the control measure (e.g. compliance with internal company rules or security interests) must be weighed against any privacy interest that the employees affected by the measure may have meriting protection and the measure cannot be performed unless found to be appropriate. The legitimate interests of the company and any interests of the employee meriting protection must be identified and documented before any measures are taken by undertaking a legitimate interest assessment (in the form of a DPIA with a particular focus on the legitimate interest). Moreover, any additional requirements under national law (e.g. works councils, rights of co-determination for the employee representatives and information rights of the Data Subjects) must be taken into account.

5.3.6 Processing of Special Categories of Personal Data

Special categories of Personal Data can be processed only if the law requires this or the Data Subjects has given his/her explicit consent. These data can also be processed if it is mandatory for asserting, exercising or defending legal claims.

5.3.7 Automated Decisions

If Personal Data are processed automatically as part of the employment relationship and specific personal details are evaluated for decision making (e.g. as part of personnel selection process or the evaluation of scores), this automatic processing cannot be the sole basis for decisions that would have negative consequences or have significant implications for the affected employee. To avoid erroneous decisions, the automated process must ensure that a natural person evaluate the content of the situation, and that this evaluation is the basis for the decision. The Data Subjects must also be informed of the facts and results of automated decisions and given the possibility to respond.

5.3.8 Telecommunications and Internet

Telephone equipment, email addresses, intranet and Internet along with internal social networks are provided by Ipsos primarily for work-related assignments. They are a tool and a company resource. They can be used within the applicable legal regulations and internal company policies, in particular the Information Security Policy. In the event of authorised use for private purposes, the law on secrecy of telecommunications in the relevant national telecommunication laws must be observed, if applicable.

Ipsos is utilising web-filtering technology and other defensive technologies for ensuring compliance with its Acceptable Use Policy, internet traffic measurement and analysis, other legal compliance obligations and to defend against attacks on the IT infrastructure or individual users. Protective measures can be implemented for the connections to the Ipsos network that block technically harmful content and for analysing the attack patterns. For security reasons, the use of telephone equipment, email addresses, the intranet/Internet and internal social

networks can be locked permanently or on a temporary basis for individual addresses/locations or connection types. Evaluations of this data from a specific person can be made only in a concrete, justified case of suspected violations of law or policies of the Ipsos Group or an immediate threat to the IT infrastructure and has to be authorised by any of the persons who may authorise a “legal hold” (see also the Information Management Policy). The relevant national laws must be observed in the same manner as the group regulations.

5.4. Marketing Contacts

Generally, marketing contacts are no different than respondents in respect of the privacy protections accorded to them. Their contact details constitute Personal Data, even if they are business related. Only if the contact details are truly generic like “contact@acme.com”, will they not fall under this Policy.

Marketing communications are often subject to specific legal requirements, particularly if they are sent electronically or made by phone.

It has to be assumed, that marketing contacts have not requested the marketing materials. In other words, the recipients have not requested to receive marketing communications from Ipsos. To proceed legally, the conditions concerning legal basis, in particular, consent requirements set out in paragraph 1 apply here as well.

Exceptionally a 'soft opt-in' can be applied, if the below conditions are met:

- where the Data Subject’s details were obtained in the course of a sale or negotiations for a sale of Ipsos services;
- where the messages are only marketing similar services;
- where the person is given a simple opportunity to refuse marketing when their details are collected; and
- at the time of the first marketing communication the right to object is brought to the explicit attention, present clearly and separate from other information, and they are given a simple way to do so in all future messages.

6. Transmission of Personal Data

Transmission of Personal Data to recipients outside or inside the Ipsos Group is subject to the authorisation requirements for processing Personal Data under paragraph 4.7 Restriction on Transfers. The data recipient (be this another Ipsos company or any supplier) must be required to use the data only for the defined purposes. For external transfers to suppliers, the requirements of this paragraph and those of paragraph 7 Outsourced/Third Party Data Processing apply cumulative.

If Personal Data are transmitted to a recipient outside the Ipsos Group, this recipient must agree in writing to maintain a data protection level equivalent to this Data Protection Policy or as required under applicable law. For example, the GDPR stipulates various requirements that must be complied with, before any transfer may occur. This does not apply if transmission is based on a legal obligation. A legal obligation of this kind can be based on the laws of the domiciliary country of the Ipsos Group company transmitting the data. In the alternative, the laws of the domiciliary country of the Ipsos Group company may acknowledge the purpose of data transmission based on the legal obligations of a third country.

Where Personal Data are transmitted by a third party (like a sample supplier) to an Ipsos Group company, it must be ensured that the Personal Data can be used for the intended purpose.
If Personal Data are transferred from an Ipsos Group company with its registered office in one country to an Ipsos Group company with its registered office in another country, the company importing the data is obligated to cooperate with the enquiries made by the relevant

supervisory authority in the country in which the party exporting the data has its registered office and to comply with any observations made by the supervisory authority with regard to the processing of the transmitted data.

If a Data Subject claims that this Data Protection Policy has been breached by an Ipsos Group company located in another country that is importing the data, the Ipsos Group company that is exporting the Personal Data undertakes to support the Data Subject concerned, in establishing the facts of the matter and also asserting his/her rights in accordance with this Data Protection Policy against the Ipsos Group company importing the data. In addition, the Data Subject is also entitled to assert his or her rights against the Ipsos Group company exporting the data. In the event of claims of a violation, it is the exporting company's obligation to demonstrate to the Data Subjects that the company importing the Personal Data did not violate this Data Protection Policy.

Each Ipsos Group company transmitting Personal Data to an Ipsos Group company located in another country, shall remain liable for any violations of this Data Protection Policy committed by the Ipsos Group company that received the Personal Data, as if the violation had been committed by the Ipsos Group company transmitting the Personal Data.

Any transfer of Personal Data within the Ipsos Group shall only be made after a relevant entry into JobBook for the project or services under which the transfer occurs has been made. Such entry will create a contract under the Ipsos Intragroup Master Services Agreement and automatically makes the respective EU Model Clauses applicable to such transfer.

7. Outsourced/Third Party Data Processing

In many cases Ipsos is using external suppliers/providers to process Personal Data. In these cases, an agreement on data processing on behalf of Ipsos must be concluded with such provider/supplier. This can be done either by way of including appropriate provisions in the agreement governing the overall relationship with the provider/supplier or in a separate and specific document. In respect of processing on behalf of Ipsos, the provider/supplier may only process the Personal Data as per the written instructions from Ipsos. When instructing a provider/supplier, the following requirements must be complied with:

- Where the Personal Data in question fall under paragraph 5.2 (client data), any relevant client requirements need to be passed down to the provider/supplier.
- The provider/supplier must be chosen based on its ability to cover the required technical and organisational protective measures and in line with Ipsos supplier approval process.
- The provider/supplier must not subcontract the processing further without Ipsos's prior written consent.
- The instructions must be in writing by way of an appropriate contract. The instructions on data processing and the responsibilities of Ipsos and provider/supplier must be documented.
- Before the data processing begins, Ipsos must be confident that the provider/supplier will comply with its duties. A provider/supplier can document its compliance with data security requirements in particular by presenting suitable certification(s). Depending on the risks of the data processing, the reviews must be repeated on a regular basis during the term of the contract. Ipsos should retain the right to audit the provider's/supplier's compliance.
- In the event of cross-border contract data processing, the relevant national requirements for transferring Personal Data abroad must be met. In particular, the Personal Data from the European Economic Area can be processed in a third country only, if the provider/supplier can prove that it has a data protection standard equivalent to the GDPR and this Data Protection Policy. Suitable tools can be:
    - an agreement based on EU standard contract clauses for contract data processing in third countries with the provider. Similar agreements will be required for any subcontractor of the provider/supplier.
    - Participation of the provider/supplier in a certification system accredited by the EU for the provision of a sufficient data protection level.

8. Rights of the Data Subject

Every Data Subject has the rights set out in this Section, whether they are provided for under applicable legislation or not. This obviously does not affect any further or extensive rights Data Subject might enjoy under national legislation, including GDPR. Their request pursuant to these rights are is to be handled immediately by the relevant Ipsos company and may not result in any disadvantage to the Data Subject. Where the relevant Personal Data are being processed by Ipsos under paragraph 5.2 Personal Data Provided by Clients, the relevant client contract must be consulted in respect of any process to be followed and the client has to be informed about such request immediately.

- **Right of access**:
  - The Data Subjects may request information on which Personal Data relating to him/her have been stored, how the data were collected and for what purpose.
  - If Personal Data are transmitted to 3rd parties, information must be given about the identity of the recipient or the categories of recipients, including other Ipsos companies.
- **Right to rectification**: If Personal Data are incorrect or incomplete, the Data Subject can demand that they are corrected or supplemented.
- **Right to withdraw consent**: Where the Personal Data are processed on the basis of consent (see also the separate guidance on Consent), the Data Subject can object to the processing at any time. These Personal Data must be blocked from the processing that has been objected to.
- **Right to erasure**. The Data Subject may request his or her data to be deleted if the processing of such data has no legal basis, or if the legal basis has ceased to apply. The same applies if the purpose behind the data processing has lapsed or ceased to be applicable for other reasons. Existing retention periods and conflicting interests meriting protection must be observed.
- **Right to object**: The Data Subject generally has a right to object to his/her data being processed and this must be taken into account if the protection of his/her interest takes precedence over the interests of the data controller owing to the particular personal situation. This does not apply, if a legal provision requires that the Personal Data are to be processed.
- **Right to data portability**. The Data Subject has the right to request that the Personal Data held by Ipsos are provided by him/her and be made available to such Data Subject in an easily readable format, like a Word or Excel document.

9. Confidentiality of Processing

Personal Data are subject to data secrecy. Any unauthorised collection, processing, or use of such data by employees is prohibited. Any data processing undertaken by an employee that he/she has not been authorised to carry out as part of his/her legitimate duties is un-authorised. The “need-to-know” principle applies. Employees may have access to Personal Data only as is appropriate for the type and scope of the task in question. This requires a careful breakdown and separation, as well as in limitation, of roles and responsibilities, with corresponding access rights. Furthermore, the requirements of the Information Management Policy apply.

Employees are forbidden to use Personal Data for their own private or commercial purposes, to disclose them to unauthorised persons, or to make them available in any other way. Supervisors must inform the employees at the start of the employment relationship about the obligation to maintain data secrecy. This obligation shall remain in force even after employment has ended. The employment agreements with Ipsos staff must contain appropriate confidentiality obligations.

10. Privacy by Design and Default

Ipsos will use a Privacy by Design and Default approach in all its work, but in particular when:

- building new IT systems for storing or accessing Personal Data;
- developing new applications or research approaches;

- embarking on a data sharing initiative; or
- using Personal Data for different purpose(s) than for which they had been collected.

Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start. It is a key consideration in the early stages of any project, and then throughout its lifecycle.

Taking a privacy by design approach is an essential tool in minimising privacy risks and building trust and will designing projects, processes, products or systems with privacy in mind from the outset

In respect of the examples given above, the required tool for compliance is conducting a DPIA in accordance with the further guidance that can be found on the intranet.

11. Data Protection Impact Assessment

Before conducting any of the processing activities described below, a DPIA will have to be completed in accordance with the further guidance that can be found on the intranet. This is in addition to the other instances already referred to in this Policy as Ipsos business is based on large scale processing of Personal Data.

Type of processing operation(s)	**Description**
Innovative technology	Processing involving the use of new technologies, or the novel application of existing technologies (including AI). Any intended processing operation(s) involving innovative use of technologies (or applying new technological and/or organisational solutions).
Denial of service	Decisions about an individual's access to a product, service, opportunity or benefit which are based to any extent on automated decision-making (including profiling) or involves the processing of special- category data.
Large-scale profiling	Any profiling of individuals on a large scale
Biometric data	Any processing of biometric data for the purpose of uniquely identifying an individual. Any intended processing operation(s) involving biometric data for the purpose of uniquely identifying an individual
Genetic data	Any intended processing operation(s) involving genetic data.
Data (base) matching	Combining, comparing or matching Personal Data obtained from more than one source.
Invisible processing	Processing of Personal Data that have not been obtained directly from the Data Subject in circumstances where the controller considers that complying with the transparency principle (see paragraph 4.1) would prove impossible or involve disproportionate effort. Any intended processing operation(s) where the controller considers that complying with the transparency principle (see paragraph 4.1) would prove impossible or involve disproportionate effort.

Tracking	Processing which involves tracking an individual's geolocation or behaviour, including but not limited to the online environment. Any intended processing operation involving geolocation data.
Risk of physical harm	Where the processing is of such a nature that a Personal Data breach could jeopardise the health or safety of individuals.

12. Processing Security

Personal Data must be safeguarded from unauthorised access or disclosure (whether caused internally or externally), unlawful processing as well as accidental loss, modification or destruction. This applies regardless of whether the data is processed electronically or in paper form. Apart from securing existing Personal Data in line with Ipsos's relevant policies (please see the Ipsos Book of Policies and Procedures Chapter 7, which is applicable in that respect), before the introduction of new methods of data processing, particular new IT systems or research approaches, technical or organisational measures to protect Personal Data must be defined and implemented. These measures must be based on the state of the art, the risk of processing and the need to protect the data. This information will also be required for the relevant DPIA.

These technical and organisational measures should be agreed in consultation with the relevant Information Security Officer and DPO. The technical and organisational measures for protecting Personal Data are part of the Corporate Information Security management and must be adjusted continuously to technical development and advancement as well as organisational changes.

As a minimum, Ipsos will process all Personal Data it holds in accordance with its Security Policy and take appropriate security measures against unlawful or unauthorised processing of Personal Data, and against the accidental loss of, or damage to, Personal Data.

13. Data Protection Audit

Compliance with this Data Protection Policy and the applicable data protection laws is checked regularly with data protection audits and other controls. The performance of these controls is the responsibility of the CPO, the DPO's, Internal Audit and/or externally hired auditors. Various Ipsos clients also have audit rights under their agreements with Ipsos. The results of all data protection audits must be reported to the CPO and Head of Compliance. On request, the results of data protection audits will be made available to the responsible data protection authorities.

14. Data Protection Incidents

All employees must inform their DPO or the CPO immediately about cases of violations of this Data Protection Policy or other regulations on the protection of Personal Data, in accordance with the Personal Data Breach Management Procedure which can also be found in Section 8 of the Ipsos Book of Policies and Procedures. Any failure to address serious failings under this Policy can also be reported under the Ipsos Whistle-blowing system.
By way of example only, in case of:

- improper transmission of Personal Data to 3rd parties;
- improper transmission of Personal Data across borders;
- improper access, including by third parties, to Personal Data, or
- loss of Personal Data (including then becoming public due to internal failures).

a data protection breach notification must be made immediately to ensure that a) any reporting duties in respect of Data Subjects, as well as data protection authorities under national law

can be complied with, b) any affected client can be informed and c) any stakeholder communication can be managed. Any Data Protection breach will also constitute an information security incident under the IT Incident Management policy.

15. Responsibilities and Sanctions

15.1. Management

The executive bodies of the respective Ipsos Group companies are responsible for data processing in their area of responsibility. Therefore, they are required to ensure that not only the requirements under national law but also those contained in this Data Protection Policy are met (e.g. national reporting duties).

Management is responsible for ensuring that organisational, HR and technical measures are in place so that any data processing is carried out in accordance with these data protection requirements.

Compliance with these requirements is also the responsibility of the relevant employees.

If official agencies conduct data protection audits, the CPO must be informed immediately.

The relevant Ipsos country management must inform the CPO as to the name of the DPO. Improper processing of Personal Data, or other violations of the data protection laws, can be criminally prosecuted in many countries and result in claims for compensation of damage. In addition, violations for which individual employees are responsible can lead to sanctions under employment law.

15.2. Data Protection Officers

Each Ipsos country will be required to appoint one or more Data Protection Officers ("**DPO**"). The DPO's are the internal and external contact persons in country for data protection. They can perform checks and must familiarise the employees with the contents of this Data Protection Policy and applicable legislation. The relevant management is required to assist the DPO's with their efforts. The main tasks of the DPO are:

- *To inform and advise the organisation and its employees about their obligations to comply with the applicable data protection laws and this Data Protection Policy.* This task will be supported and guided by Group and through the network of DPOs under the leadership of the CPO and training.
- *To monitor compliance with the data protection laws, including managing internal data protection activities, advise (not to conduct) on data protection impact assessments; train staff and conduct internal audits.* This will be supported and guided by Group. Audits, other than spot checks, should be co-ordinated with the Group internal audit function.
- *To provide advice concerning DPIAs.* Under the DPIA a processor, the advice of the responsible it DPO has to be sought and considered as part of the assessments to be made in the DPIA.
- *To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc.).*

Within each Ipsos country, the DPO will have:

- To report to the highest management level of the Ipsos country organisation – i.e. to local management board level or member.

- To operate independently of professional orders, and is not dismissed or penalised for performing their task.
- To be provided with adequate resources to enable the DPO to meet their obligations under the applicable data protection laws and this Data Protection Policy.

The Data Protection Officers shall promptly inform the CPO of any data protection risks.

15.3. Global Chief Privacy Officer

The Global Chief Privacy Officer ("**CPO**"), being internally independent of professional orders, works towards the compliance with national and international data protection rules. He/she is responsible for this Data Protection Policy and supervises its compliance.

Any Data Subject may approach the CPO or the relevant DPO at any time to raise concerns, ask questions, request information or make complaints relating to data protection or data security issues. If requested, concerns and complaints will be handled confidentially.

If the relevant DPO cannot resolve a complaint or remedy a breach of the Data Protection Policy, the CPO must be consulted immediately. Decisions by the CPO to remedy data protection breaches must be upheld by the management of the company in question. Enquiries by supervisory authorities must always be reported to the CPO.

16. Derogation

In exceptional cases, it may be possible to obtain a derogation from this Policy, prior to any intended processing of the Personal Data affected. Any such derogation may only be granted following a full DPIA to establish and assess the risks to any affected Data Subject, legal risks and reputational impact and is subject to approval by the Ipsos President Support Services.

17. Glossary

Various expressions below have furthermore detailed definitions which can be accessed by following the links. Relevant cases are indicated by headings in *italics.*

Data Controller/Controller/Joint Controller
This is the person or organisation which determines the purposes for and the manner in which any Personal Data is processed. It is responsible for establishing practices and policies in line with the applicable legal requirements.

In most cases where Ipsos is receiving sample from client, it will be joint controller of the data collected. This extends to the data we collected, even where we have assured the respondents of the confidentiality of their answers. The responsibilities and obligations of the joint controllers have to be documented and clarified in a written agreement.
Some jurisdictions use other expressions for the same concept, like **Responsible Person**, **Organisation**, **Operator**[1] etc.

Data Users
These are those of our employees whose work involves processing Personal Data. Data users must protect the data and Personal Data they handle in accordance with this Policy and any applicable data security procedures at all times.

Data processor or Processor

[1] Singapore

This is the person or organisation that is not a Data User that processes Personal Data on behalf and on instructions of the Controller. Employees of data controllers are excluded from this definition, but it includes suppliers which handle Personal Data. Ipsos will variously be a Controller (e.g. in respect of our panellists or ad-hoc sample Ipsos recruits for a survey) or a Processor (e.g. in respect of sample provided by clients). Some jurisdictions use other expressions for the same concept, like **Third Party, Intermediary**, **Operator**[2] etc.

Data Subjects

For the purpose of this Policy include all living individuals about whom an Ipsos Company hold Personal Data. A Data Subject need not be a country's national or resident. All Data Subjects have legal rights in relation to their Personal Data.

Personal Data

The GDPR's definition of Personal Data (GDPR Article 4 (1)) makes it clearer what Personal Data are and shows that this must be widely interpreted:

"…any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

It is important to note that **all** data about a Data Subject are Personal Data, not just the data identifying him/her.

A natural person is a living individual and the GDPR itself does not apply to deceased individuals. However, individual member states may provide for rules concerning the processing of Personal Data even in respect of deceased persons.

Information about a company will not constitute Personal Data.

It is not always possible to determine with absolute certainty, whether an individual item of information would constitute Personal Data. It will be necessary to look the overall information held about the person in question or the means reasonably likely to be used to identify a person. With the ever improving technological means, more data will become Personal Data.

Processing

Processing generally is any activity that involves use of the data. More specifically in relation to data protection it is any operation or set of operations which is performed on Personal Data or on sets of Personal Data. It includes collecting, organisation, structuring, storing, adapting or altering, obtaining, recording, holding organising, amending, retrieving, using, disclosing, erasing or destroying Personal Data. Processing also includes transferring Personal Data or accessing them, irrespective from where this might be.

Special categories of data (p/k/a personal sensitive data)

"Special categories of Personal Data" is the new expression used in the GDPR and was previously referred to as "sensitive data". This is now defined in Article 9 GDPR as data concerning the:
racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data [see below], biometric data [see below] for the purpose of uniquely identifying a natural person, data concerning health [see below] or data concerning a natural person's sex life or sexual orientation

[2] South Africa

For some of these expressions more detailed definitions have been provided in the GDPR:

'genetic data' means Personal Data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

'biometric data' means Personal Data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

'data concerning health' means Personal Data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

Anonymous Data

This has been defined as information which does not relate to an identified or identifiable natural person or to Personal Data rendered anonymous in such a manner that the Data Subject is not or no longer identifiable (GDPR Recital 26). This must be distinguished from data which, together with the use of additional information (e.g. a key), could be used to identify a natural person, then the data were merely pseudonymised.
Pseudonymised data still fall under the definition of Personal Data and full GDPR principles and requirements will still apply to them.

Pseudonymisation

Pseudonymisation means the processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the Personal Data are not attributed to an identified or identifiable natural person. (GDPR Article 4(5))
Pseudonymous data refers to a data from which identifiers in a set of information are replaced with artificial identifiers, or pseudonyms, that are held separately and subject to technical safeguards. Pseudonymised data remain Personal Data and therefore all other data protection requirements continue to apply to them!!

PII or Personally Identifiable Information

This term derives from US privacy legislation. It only covers a narrow element of Personal Data as it is focused on those data identifying a Data Subject, whereas Personal Data applies to all data relating to data subject. The use of the expression PII in the context of this Policy has to be avoided, as it otherwise negatively impacts on our obligation to demonstrate compliance.

PHI or Protected Health Information

This term also derives from US privacy legislation, in particular HIPAA in the US. Although from a practical perspective applicable to Ipsos's day-to-day working the expressions special categories of Personal Data and PHI should be treated as synonymous, the use of PHI in the context of this Policy should be avoided.

The main issue to be considered is, that a certain Personal Data that would fall under the legal definition of PHI, under GDPR would constitute Personal Data rather than special categories of data. For example, HIPPA would consider all information in a dataset that were to contain the name and sexual

orientation as PHI, whereas the GDPR would only consider the sexual orientation to be part of the special categories of Personal Data.

PSI or Personal Sensitive Information

This expression is now outdated, having derived from previous legislation. This is largely synonymous with "special categories of Personal Data", and this latter expression should be used. Regulators will expect Ipsos to use the correct terminology to demonstrate our compliance as part of our accountability obligation.