Ipsos Nigeria Privacy & Data Protection Policy

(Effective 25 October 2019)

Ipsos Nigeria Privacy & Data Protection Policy

Contents

1. Introduction

As part of its social responsibility, Ipsos Nigeria Limited ("Ipsos" or "Ipsos Nigeria") is committed to national and international compliance with data protection laws, regulation and rules. This privacy & data protection policy ("**Policy**" or "**Data Protection Policy**") applies to Ipsos Nigeria Ltd and is based on globally accepted basic principles on data protection. This Policy adopts the fundamental principles of the Nigerian Data Protection Regulation 2019 (NDPR) as the minimum standard to which Ipsos, its employees and suppliers must adhere.

Ipsos depends on the collection and analysis of information about natural persons ("**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) 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 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 the 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 to Ipsos Nigeria. Within Ipsos, this Policy will form the minimum standard to which all Ipsos, employees and suppliers must adhere, regardless of whether NDPR 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, Regulations and Codes of Conduct

This Data Protection Policy adopts the internationally accepted privacy principles as enhanced by the NDPR. 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 be observed. The contents of this Policy must also be observed in the absence of corresponding national legislation.

Ipsos is responsible for compliance with this Data Protection Policy and applicable legal obligations.

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 NDPR

Ipsos regards the lawful and correct treatment of Personal Data and maintaining the confidence of those with whom it deals as a vital component of its business operations and is committed to act ethically and responsibly in respect of these Personal Data and to provide always 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 NDPR Ipsos respects the following principles, which are explained in more detail later, concerning Personal Data and that they are:
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 data 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. 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 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 possible to a limited extent and require substantiation and validation. The 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.

4.3. 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 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 with the goal being pursued, 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 accurate, 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.

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, pseudonymised data must be used for the processing – REMINDER: pseudonymised data remain and are Personal Data!

4.7. Restriction on Transfers

Personal Data must not be transferred to other countries (even to other Ipsos companies in such 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 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 giving a statement or by a clear affirmative action, signifies 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, their Personal Data may be processed where this is necessary in the context of a contract to which such Data Subjects is a party, to fulfil 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.

5.1.3. Data Processing Pursuant to Legal Authorisation

The processing of Personal Data is also permitted where legal obligation or compliance requires or allows its. This type and extent of data processing must be necessary for the legally authorised data processing activity and must comply with the relevant statutory provisions.

5.1.4 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 please see the intranet. Special categories of Personal Data can also be processed if it is mandatory for asserting, exercising or defending legal claims. Special categories of Personal

Data may be further processed for scientific and historical research and for statistical purposes (Paragraph 2.1(1)((a)(i) of the NDPR , subject to appropriate additional measures. Before relying on this provisions, the advice of the DPO must be obtained.

5.1.5 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 easy to identify, 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 upon explicit consent of the Data Subjects. Even if tracking uses a pseudonym for the Data Subject, the Data Subject should be given the chance to opt out in the privacy statement. In respect of online audience measurement without prior opt-in, Ipsos also adheres to the principles promulgated by researchchoices.com.

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 Guide on Social Media Research, 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.

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 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 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;
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 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 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 the 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.
It may be necessary during the application procedure to collect information on an applicant from a third party. 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 or consent of the employee.

5.3.2. Data Processing Pursuant to Legal Authorisation

Please see above at paragraph 5.1.3 for the further 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. Involuntary consent is void. To the extent that consent is a valid basis for processing, please see above at paragraph 5.1.1 for the further requirements. A further complication is, that consent can normally be withdrawn, thereby preventing any further processing.

5.3.5 Processing of Special Categories of Personal Data

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

5.3.6 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 create significant problems 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 individual decisions and the possibility to respond. The 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.

5.3.7 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 & Acceptable Use Policy. In the event of authorised use for private purposes, the law on protection of consumer information under the Nigerian Communication Commission Act must be observed..

Ipsos is utilising web-filtering technology 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 and has to be authorised by any of the persons who may authorise a “legal hold” (see also the IT Information Management Policy).

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 asked to receive marketing communications from Ipsos. To proceed legally, the conditions concerning legal basis, in particular, consent requirements set out in paragraph 5.1.1 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; and
- where the person is given a simple opportunity to refuse marketing when their details are collected, and if they don't opt out at this point, are given a simple way to do so in all future messages.

6. Transmission of Personal Data

Transmission of Personal Data to recipients outside Ipsos 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 sub-contractor) must be required to use the data only for the defined purposes. For external transfers 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 of Ipsos to a third country, 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 NDPR stipulates various requirements that must be complied with, before any transfer may occur. This does not apply if transmission is to a country that is on the White List of Countries issued by NITDA or where the transmission is based on:

a) explicit consent of the Data Subject to the proposed transfer, after having been informed of the possible risks of such transfers;

b) performance of a contract between the Data Subject and the Controller or the implementation of pre-contractual measures taken at the Data Subject's request;

c) the conclusion or performance of a contract concluded in the interest of the Data Subject between the Controller and another natural or legal person;

d) important reasons of public interest;

e) the establishment, exercise or defence of legal claims; and

f) the protection of the vital interests of the Data Subject or of other persons, where the Data Subject is physically or legally incapable of giving consent;

Where Personal Data are transmitted by third party (like a sample supplier or a member of the Ipsos group of companies) to Ipsos, it must be ensured that the Personal Data can be used for the intended purpose and all country laws or regulations have been complied with.

If a Data Subject claims that this Data Protection Policy has been breached by Ipsos we undertake 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 In the event of claims of a violation, Ipsos will document to the Data Subjects that the company importing the Personal Data did not violate this Data Protection Policy.

When transmitting Personal Data to an Ipsos Group company located outside Nigeria we 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 Ipsos.

7. Outsourced/Third Party Data Processing

In many cases Ipsos is using external processors to process Personal Data. In these cases, an agreement on data processing on behalf of Ipsos must be concluded with such processor. This can be done either by way of including appropriate provisions in the agreement governing the overall relationship with the processor or in a separate and specific document. In respect of processing on

behalf of Ipsos, the processor may only process the Personal Data as per the instructions from Ipsos. When instructing a processor, 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.
- The processor 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 processor must not subcontract the processing further without Ipsos's prior written consent.
- The instructions must be placed in writing by way of an appropriate contract. The instructions on data processing and the responsibilities of Ipsos and processor must be documented.
- Before the data processing begins, Ipsos must be confident that the processor will comply with its duties. A processor can document its compliance with data security requirements in particular by presenting suitable certification. Depending on the risk of 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 processor's compliance.
- In the event of cross-border contract data processing, the provision of the NDPR for disclosing Personal Data abroad must be met. In particular, the Personal Data from Nigeria can be processed in a third country only, if the processor can prove that it has a data protection standard equivalent to the NDPR.

8. Rights of the Data Subject

Every Data Subject has the following rights. Their request 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 Subjects 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 Subjects 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 data to be processed. The employment agreements with
- **Right to data portability**. The Data Subject has the right to request for the Personal Data provided by him/her to be made available to such Data Subject in a 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. 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 data for new purposes.

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 Data Protection Impact Assessment.

11. 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.

These technical and organisational measures should be agreed in consultation with the 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.

12. 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 DPO's, Internal Audit and/or our Data Protection Compliance Organisation. Various Ipsos clients also have audit rights under their agreements with Ipsos. The results of the 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.

13. Data Protection Incidents

All employees must inform the DPO 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.

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 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.

14. Responsibilities and Sanctions

14.1. Management

The executive bodies of Ipsos are responsible for data processing. Therefore, they will ensure the legal requirements, and those contained in this Data Protection Policy, for data protection are met.

Management are 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 employees.

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

14.2. Data Protection Officers

Ipsos will appoint a Data Protection Officers ("**DPO**"). The DPO is the internal and external contact persons fordata protection. The DPO can perform checks and must familiarise the employees with the contents of this Data Protection Policy and applicable legislation. The management shall assist the DPO's with their efforts. The main tasks of the DPO are:

- *To inform and advise the Ipsos 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 Ipsos Group and through Ipsos Group 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 Ipso Group. Audits, other than spot checks, should be co-ordinated with the Ipsos Group internal audit function.
- *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.

14.3. 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 regulators. 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.

15. 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 data protection impact assessment 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.

16. Glossary

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.

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

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 could include 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).

Data Subjects

For the purpose of this Policy include all natural persons (being Nigerians or foreigners resident in Nigeria) about whom Ipsos hold Personal Data. A Data Subject need not be a countries national or resident. All Data Subjects have legal rights in relation to their personal information.

Personal Data

The NDPR's definition of Personal Data (Paragraph 1.3(xix) of the NDPR) makes it clearer what Personal Data are and shows that this must be widely interpreted:

"Personal Data means 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 can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifier such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM, Personal Identifiable Information (PII) and others;"
A natural person is a living individual and the NDPR itself does not apply to deceased individuals.

Information about a company will not constitute Personal Data.

One has to acknowledge that 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 is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring Personal Data.

Sensitive Personal Data (Special categories of data)

The NDPR defines sensitive special data as:

''data relating to religious or other beliefs, sexual orientation, health, race, ethnicity, political views, trades union membership, criminal records or any other sensitive personal information; ''

Anonymous Data

This are 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. 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.

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.

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

The NDPR defines PII as:
''information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in a context''.

Document Control

Version	Date	Summary of Changes	Authors	Approved by
1.0	12.04.2018	Version approved for publication	Rupert van Hullen	**Laurence Stoclet**

Document review	
Last Review date	12.04.2018
Reviewed Version	1.0
Proposed changes **(list chapter no and short description of changes)**	N/A
Review Committee	CPO, GC, CIO, MarCom
Approval Authority/Committee	Deputy CEO & CFO
Next Review Due Date	12.04.2019
Note: Records within this table will not generate a change in the version number.	