Ipsos iris Privacy Policy

Purpose statement for Ipsos iris Panellists

Ipsos MORI will deliver a single source of high quality and accurate data on a daily basis through the Ipsos iris project to become the trusted and credible partner for the delivery of Online Audience Measurement for UKOM (UK Online Measurement Ltd), the media and advertising industry, websites and apps. Ipsos MORI will ensure the Privacy compliance of Panellists by…

Clarifying the Data Controllers and Processors to allow the panellist clear visibility of who owns their personal data across all the channels used within the Ipsos iris project.

The panellist's rights will be clearly stated in the relevant Controller's Privacy Notice, to include clarity on the legal reason for collection of all personal data, the secure control of sensitive data and website cookies/ tagging. Ipsos MORI will give contractual clarity, clearly define the Privacy controls required of its Processors and will work with any joint controller to establish a clear demarcation between the parties allowing full visibility to the Panellist. Ipsos MORI have proactively completed a Data Privacy Impact Assessment, which will be made available to any parties of interest ensuring full transparency of the Ipsos iris solution.

Topics

Ipsos iris Panel overview

Ipsos iris is the official source of Online Audience Measurement in the UK. The Ipsos iris Research Panel has been set up by Ipsos MORI in conjunction with UKOM in order to provide a total view of how people in the United Kingdom use the internet.

Ipsos iris is a Research Panel of 10,000 individuals from all over the United Kingdom who agree to take part in the research. By joining the Ipsos iris panel, individuals allow Ipsos MORI, in a safe and secure way, to measure what websites they visit and what apps they use every day.

Ipsos iris collects data from Smartphones, Tablets and Computers from all 10,000 panel members to build a full and comprehensive view of how people use these devices and which websites and apps they use. The aggregate research data collected is used by website owners, publishers, media producers, advertising agencies and broadcasters to ensure they continue to deliver relevant and appropriate content for their visitors.

How we use your information

Ipsos MORI UK Limited, (“Ipsos MORI”,” we” or “us”), commonly known as Ipsos MORI, is a company registered in the United Kingdom at 3 Thomas More Square, London, E1W 1YW under company number 01640855. Ipsos MORI is part of the Ipsos worldwide group of companies.
This privacy policy explains how we use any personal information we collect about you (“Panellist”, ”you” or “your”) when you:

- install the Ipsos iris app/VPN/browser extension on your primary and any additional devices,
- join our Ipsos iris panel,
- take part in Ipsos iris surveys or
- use the panel members’ website.

What personal data do we collect about you under what legal basis for processing?

Ipsos MORI, as the data controller of the Ipsos iris panel, requires a legal basis to process your personal data. Ipsos MORI’s legal basis for processing your panel data is your consent to join the panel and participate in its research activities. If you wish to withdraw your consent at any time, please see the section below covering ‘Your Rights’.

Ipsos MORI will collect the information you provide when you agree to participate in this research project, including your mobile phone number, email address and other contact details. Ipsos MORI will also automatically collect information via the:

- Ipsos iris blue App
- Ipsos iris orange App
- Ipsos iris orange browser extension
- Ipsos iris orange VPN

For panel members, the information is collected by telephone or via an online questionnaire (your phone number and email address), by completing our recruitment questionnaire when you decide to join our panel and through the Ipsos iris blue App, Ipsos iris orange Apps, Ipsos iris orange browser extension and Ipsos iris orange VPN. We may also collect information when you voluntarily complete any other panel related surveys, give your consent to cookies and tagging from certain websites, participate in any other panel activities, when you contact us, when we contact you or when you provide feedback, comments or other information to us.

In the case of the registration process (screening questionnaire, follow-up questionnaire and installation of all required devices) not being successfully completed, your information will be retained by us to prevent any fraud or misuse.

In some instances, concerning our research, we may ask you to provide certain sensitive personal data, for example revealing your racial or ethnic origin, political opinions, religious or philosophical beliefs. You do not have to answer these questions and such questions will always include a "prefer not to answer" option.

When you give your consent for us to use your data, you allow us to use and retain any data you provide. This data will be pseudonymised, and later anonymised, to protect your privacy during the length of the Ipsos iris project.

When working with partners, such as PAMCo, we will always pseudonymise the data to protect your rights, However, both Ipsos MORI and our partners may merge your data with other data sources for research purposes only. Please note, we pseudonymise this information before it is passed to any 3rd parties to maintain your privacy and they will not be able to link information to individuals.

The Ipsos iris App/VPN/Browser extension is installed for the purpose of market research. The App/VPN/Browser extension runs in the background whilst you're using your device(s) normally. They allow Ipsos MORI to collect information about the device and how you use it.

The information collected by our App/VPN/Browser extension is described below in more detail.

With the exception of any terms entered into a web search, our App/VPN/Browser extension does NOT collect keystrokes or information that is entered into a web form, such as website user IDs, passwords, credit card numbers, other financial account numbers or any other data presented on or entered into a secure (HTTPS) webpage. As a result, the App/VPN/Browser extension will normally not have access to any information regarding items in a website shopping basket or your interactions with financial or health-related websites that you may log into, as these are normally secure sites.

However, in the event that any such sensitive data is collected by mistake, such as the collection of personal data by a badly designed website (e.g. user ID/password in the URL); we can assure you any such data will be securely deleted from our systems as soon as it is found to have been collected in line with Ipsos MORI's data protection and information security policies and procedures.

The App/VPN/Browser extension will collect the URL (e.g. www.google.co.uk) of any secure (i.e. HTTPS) websites, together with any search terms you enter into a secure site that the site adds to the URL (full web address). The App/VPN/Browser extension does NOT collect information displayed in the website pages, nor any information entered into online forms (e.g. online payment form).

Information collected by our Apps/VPNs

Panel members will be invited to download and install one or more of Ipsos's research Apps/VPNs/Browser extensions. We can reassure you that these apps DO NOT record any phone calls, nor do they collect the content of any emails or text messages. The Apps/VPNs/Browser extensions used with this panel are as follows:

Ipsos iris blue App – installed on Android smartphones

The Ipsos iris blue App runs in the background whilst you're using your smartphone. It allows Ipsos MORI to collect the following information about websites/apps accessed, details on the device and how you use it:

- The GPS location of the device and if the device is moving
- The audio signal of some TV and Radio stations that identifies the station and the time that you view or listen to each one. (This function is switched off by default, however the mic will switch on occasionally to keep the app running. No conversations or personal information will ever be recorded or stored).
- Data about the date and time the device is switched on, when it uploads data, when the screen is active and the battery charge level
- When it connects to a network and what type of connection is used (e.g. a Wi-Fi connection or mobile service provider)
- Information about your device: Android Advertiser ID, together with other Information about your mobile device, such as when and for how long you charge it, how much battery power is left, whether it is switched on or off, in sleep mode and when the screen is locked or the device is active. The information about the device includes make and model
- Information about your usage of other apps and features (such as the camera, though we do not collect any photos) on your mobile device, including the identity of the apps and features, when you downloaded them, how often you use them and for how long.
- Operating system capabilities to view the contents of your applications such as Accessibility services.
- Network information: Information about which mobile network(s) you connect to, the locations of the mobile network sign tower used to connect, signal strength and at what times you connect and use them. It also records the amount of data sent or received by your device during each data collection period.

- Presence of Wi-Fi connectivity: we check if you are connected to wi-fi, but we do not collect any information about which wi-fi signal you are connected to
- Time spent using the internet, including:
    - Websites/Apps visited/used
    - How websites are accessed (e.g. Navigated to it, redirected to it or clicked on a hyperlink)
    - Reporting on the in-app content consumption of Netflix, YouTube, Amazon Prime Video, BBC iPlayer and BBC Sounds, plus potentially Spotify in the future
    - Information on Subscription Video on Demand (SVOD) capture
    - Total amount of online data usage
- Information we can deduce from combining the above information – e.g., what apps you were using just before you searched for particular information using your mobile device's internet browser, or how often you call, email or text, or the geographic location in which you are most likely to charge your device, make a telephone call, or download an app.

We may ask you to participate in additional research projects from time to time that would require the continuous use of the microphone. Your consent will be required to do this, and additional incentives would be paid for your participation.

Ipsos iris orange App – Installed on Android Tablets

The Ipsos iris orange App runs in the background whilst you're using your Android tablet. It allows Ipsos MORI to collect the following information about websites/apps accessed, details on the device and how you use it:

- Information about your device: such as when and for how long you charge it, how much battery power is left, whether it is switched on or off, in sleep mode and when the screen is locked, or the device is active. The information about the device includes make, model, its IMEI or UID and operating system
- Information about your usage of other apps and features (such as the camera, though we do not collect any photos) on your mobile device, including the identity of the apps and features, when you downloaded them, how often you use them and for how long.
- Operating system capabilities to view the contents of your applications such as Accessibility services.
- Time spent using the internet, including:
    - Websites/Apps visited/used
    - How websites are accessed (e.g. Navigated to it, redirected to it or clicked on a hyperlink)
    - Reporting on the in-app content consumption of Netflix, YouTube, Amazon Prime Video, BBC iPlayer and BBC Sounds, plus potentially Spotify in the future
    - Information on Subscription Video on Demand (SVOD) capture
    - Total amount of online data usage

Ipsos iris orange VPN – installed on iPhones and iPads

The Ipsos iris orange VPN runs in the background whilst you're using your iPhone or iPad. The IOS root certificate itself doesn't capture anything on its own, but it enables the collection of HTTPS traffic from the VPN, so in effect the two technologies come together.

The VPN will collect everything that is sent via the internet, so in effect all network traffic from the app and web usage. However, we'll only collect secure HTTPS traffic for the data points we are interested in e.g. browser activity, content level data from Netflix, iPlayer etc. We don't collect data from apps or services that don't require an internet connection i.e. calendar, calculator, phone or other default phone services.

It allows Ipsos MORI to collect the following information about websites/apps accessed, details on the device and how you use it:

- Time spent using the internet, including:
    - Websites/Apps visited/used
    - How websites are accessed (e.g. Navigated to it, redirected to it or clicked on a hyperlink)
    - Reporting on the in-app content consumption of Netflix, YouTube, Amazon Prime Video, BBC iPlayer and BBC Sounds, plus potentially Spotify in the future
    - Information on Subscription Video on Demand (SVOD) capture
    - Total amount of online data usage

NOTE: you may see a message that pops up when you install the browser extension, it is a default message generated by the operating system to explain what the extension is technically capable of capturing, such as passwords etc. However, we do not configure our extension to do this. So, our Privacy Policy document explains what we actually capture.

We do not collect any sensitive data such as bank accounts or account logins

Ipsos iris orange browser extension – installed on Computers (Mac & PC)

The Ipsos iris orange browser extension runs in the background whilst you're using your computer. It allows Ipsos MORI to collect the following information about websites/apps accessed, details on the device and how you use it.

- Time spent using the internet, including:
    - Websites/Apps visited/used
    - How websites are accessed (e.g. Navigated to it, redirected to it or clicked on a hyperlink)
    - Reporting on the in-app content consumption of Netflix, YouTube, Amazon Prime Video, BBC iPlayer and BBC Sounds, plus potentially Spotify in the future
    - Information on Subscription Video on Demand (SVOD) capture
    - Total amount of online data usage

Applications that are "Screened Out", Duplicated, Fraudulent or Not Completed Properly ("Speeders")

- During the onboarding process, we may lose some candidates, due to:
- candidates being screened out, as per the "Membership" section in the T&Cs
- completion of duplicate applications
- attempts to complete the application in a fraudulent manner
- incomplete, or too hastily addressed, applications, also known as "Speeders"

When these occur the individual will not be allowed to participate as a panellist and their details will be removed, but kept for reference in case of future attempts to join the panel. NOTE: No incentives will be provided for the above scenarios

Use of Project by children

We understand the importance of protecting the privacy of minors, especially in the online environment. This Ipsos iris project is not designed for or intentionally targeted at minors under the age of 15. We will always gain the consent of anyone aged younger than 16 from their Parent or Guardian. If we become aware that we have collected personal information relating to a minor, we will take reasonable steps to delete it.

Why we collect information from you

The primary purpose of collecting information from you is for Ipsos MORI to conduct market research. When you join our Panel or install any of our Apps/VPNs, we enter into a contract with you, which is subject to this Privacy Policy as well as our Terms and Conditions.

In order to fulfil this contract, we need to collect, process and collate the information requested during the recruitment or that we subsequently collect in accordance with this Privacy Policy and process it. This information will be used to contact you concerning the Ipsos iris project, which is also explained in more detail in our Terms and Conditions.

Where you install any of our Apps/VPNs, respond to any survey invitations we might be sending you or that you may otherwise voluntarily provide. Your participation is at your choice. There might also be situations where we are seeking further information from you or even explicit consent where this might be appropriate or required.

The overall operation and how the Panel works is described in more detail in our Terms and Conditions **Here.**

When you request deletion, leave or are removed from the panel, we will remove the link between your profile information and the responses you provided before deleting your record. We will only

keep a minimise version of your data to uniquely identifying you as a “removed panellist” to prevent duplication or fraudulent activity.

The anonymous research data will be retained within our records for the duration of the project.

Use of Cookies and Page Tagging

A cookie is a small text file that is stored on a user’s computer for record-keeping purposes. We use cookies on our site www.irispanel.ipsos.com. We do not link the information we store in cookies to any personally identifiable information, including the email address, you submit while on our site. We use session cookies to make it easier for you to navigate our site, some websites within the Ipsos iris project may also contain web tags or website tags which are a tool used to gather data on a website.

See below for more information on our use of Cookies contained in our Research Network, which is run by our trusted partner, DotMetrics:

- **DeviceKey internet cookie** (ends with session)
  This internet cookie collects information about the data subject's device. The purpose for which we use it is to provide a high-quality view of the survey or some content on the data subject's device.
- **Session Temp internet cookie** (ends with session)
  With this internet cookie, we obtain information about a visit to the Research Network.
- **Session Temp Timed internet cookie** (ends with session)
  Contains information about the current site from which you access the Research Network.
- **Unique User Identity internet cookie** (30 days)
  Contains information about the current user e.g. your unique ID, creation time, current tracking mode and version
- **Site Id internet cookie** (ends with session)
  Indicates which site or what site category is measured.

NOTE: This privacy statement covers the use of cookies by Ipsos Panels only and does not cover the use of cookies by any third parties.

Use of Digital Fingerprinting

We also use digital fingerprint technology, also known as "Machine Identification", to gather certain information about your computer, hardware and software, such as:

IP address / display settings of your monitor / type of browser used / type of operating system

This information is sent to our trusted provider, Dotmetrics, who converts it into a unique serial number (the digital "fingerprint") and determines if it matches previous fingerprints. The data collected in this process and the digital fingerprint created are not tied to any of your personal information and are stored on secured servers.

How do we use your information?

We will use your information for our ongoing research into how people use various devices to access the internet and interact with websites and Apps.

The results of this research will be fully anonymous statistical research data only. You will NOT be identifiable in any published results.

We will use the information you provide to:

- Fulfil our contract with you
- Keep a record of all Panellists
- Respond to any messages, questions or issues you may raise
- Allow you to sign up with our rewards partner to provide any incentives offered to you for assisting with this research
- Send you invitations to participate in surveys that are relevant to you based on the information you provided in response to our recruitment questionnaire(s) or as may be updated by you at a later stage
- Contact you via SMS message to your mobile phone number (if applicable) containing a verification code, to verify your application and activate your Panellist account;
- Contact you via SMS, email or telephone regarding the completion of the software installation and signup process.

- Contact you via SMS, email or telephone regarding any issues we are having receiving data from you or if you stop sending data or send less than the minimum amount of data
- Append existing personal information about you to your responses to any market research you participate in, such as geographical location, ethnicity, occupation categories etc. for survey analysis of the responses and producing anonymous, statistical research results
- Enter you into any prize draws that you are eligible to take part in or, where invited to do so, have asked to be entered
- With your explicit consent, which might be sought in a specific survey and limited thereto, to pass your individual data together with your personal information to the client who commissioned the research. The client will use this information only for research purposes as explained in the relevant survey.
- Where you have explicitly consented, Ipsos MORI may contact you to participate in further research projects they conduct separately and prior to your information being provided to the client for this, the client may also use this information to contact you to invite your participation in further research they conduct;
- To create anonymous, statistical profiles of the Panel membership based on the information provided by Panellists;
- With your consent, to pass your information to other Ipsos Group companies so that they may invite you to participate in research studies they are carrying out and that may be relevant to you; and
- Send you by email newsletters, announcements and other communications as set out in the Terms and Conditions.
- Where you agree to take part in a product test to arrange for such a product to be sent to you.
- If you have become a member of the panel through one of our third-party recruitment suppliers, they will be informed that participants have completed the screening questionnaire.

Note: Ipsos MORI enforces procedures in order to select suppliers processing personal data based on their capacity to comply with Ipsos MORI's data protection requirements. This means that all suppliers must sign an agreement with Ipsos MORI including data protection clauses at least as strict as the ones Ipsos MORI signs with its customers, and that no supplier can transfer any personal data outside the EEA unless they agree to appropriate safeguards and obtain customer consent. Additionally, our suppliers cannot subcontract part of the personal data processing services to sub-processors without Ipsos MORI's prior approval

As part of our online advertising research and internet usage research studies, we may also:

- Send you invitations by text message (if applicable) to take part in additional research.
- If required, we may also ask you to participate in additional research about what TV channels you watch and what Radio stations you listen to. This will require your consent to access the mic on your device to detect the Audio signal from TV and Radio. No conversations will ever be recorded or stored

We may also send your information to our sub-contractors or affiliated companies, listed in the table below, who carry out some work on our behalf, around, control and responsibility for data hosting or as described above.

Sub-contractors	Website
RealityMine	https://www.realitymine.com/
Intrasonics	https://www.intrasonics.com/
IDM	https://www.idmgroup.com/
BI Worldwide	https://www.biworldwide.co.uk/
DotMetrics	https://www.dotmetrics.net/

Some of these sub-contractors may be based outside the European Economic Area; however, they are required to abide by the same data privacy legal requirements and security arrangements as ourselves and will be subject to appropriate safeguards, a description of which can be obtained by contacting us from the details at the bottom of this document.

We will take all reasonable steps to ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which they were obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless you have consented to this.

We will NEVER use your information for any purpose other than research or as described in this policy. Other than in relation to this Panel (like participating in further surveys), we will NOT try to sell you anything, nor use your information for marketing purposes, nor will we pass your information to third parties for marketing or advertising purposes. We will not add information to the data record we collect to try to profile you as an individual,

For more information about our Panel, Panel membership or information related to your membership of our panels, please contact our Panel Support Team. They can be contacted as set out in the details at the bottom of this document.

Who will have access to your information?

Your information may be processed by:

Those Ipsos MORI staff involved in this research project, or who need access in order to directly support the systems used. This may include staff in:

- Other Ipsos Group companies involved in this research, some of which may be located in other countries. The data will be moved safely and will always be pseudonymised.
- Our sub-contractors who may carry out some of the processing on Ipsos MORI's behalf, and under Ipsos MORI's control; for example: the service providers who host or provide technical support for our systems.
- As of 6th August 2020, our sub-contractor, BI Worldwide, will provide the monthly incentives for the panellists, albeit with the data being pseudonymised, and the panellists being asked to register directly with BI Worldwide.
- Where required by law or regulation, we may be required to disclose some of your information to relevant authorities; for example, if you are being investigated by the police for criminal activity.
- It may be that Ipsos MORI is a joint controller with the data collector in which case you should be aware of their Privacy Notice and give explicit consent, or agree to lawful processing under legitimate interest, for them to use your personal data for the stated purpose(s).

This may also involve transferring your personal information to other countries, including the USA and India. However, we can reassure you we take great care to ensure any transfers are carried out securely and in compliance with all applicable data protection and data privacy legal requirements through a set of Binding Corporate Rules for all companies under the Ipsos Company Group. We can also assure you that any sub-contractors involved are also required to abide by the same contracted data privacy legal requirements and security arrangements as Ipsos MORI.

What we do to keep your information secure

We take very seriously our responsibilities to keep your personal, and sensitive, information secure. As such we take every reasonable precaution to ensure your information is protected from loss, theft or misuse. These precautions include appropriate physical security of our offices, controlled access to computer systems, and use of secure, encrypted internet connections when collecting personal information. Ipsos MORI have the ISO27001 and Cyber Essential accreditation standards to ensure a safe and secure infrastructure. Ipsos MORI will continually review and improve its information security measures to ensure they continue to effectively support the business and remain compliant with our legal, regulatory and contractual obligations.

How long will Ipsos MORI keep your information?

We will keep the profile information you provided for as long as you remain a Panellist.

NOTE: You can leave the Panel at any time you wish.

When you leave the panel or are removed, we will retain only the minimum required personal data to uniquely identify you as an individual, for the sole purpose of preventing any duplicate or fraudulent participation for the duration of the panel, unless you specifically request that we delete all your personal data in accordance with GDPR Article 17

Apart from your profile information, Ipsos MORI will also gather the answers you give in any survey. The answers provided by you will be pseudonymised by Ipsos MORI for security reasons and will only be shared with our clients in this form unless you have given your explicit consent to you being

identified. We will also remove the link between your profile information and the answers you provided within 12 months of the end of the research project, to ensure that these answers cannot be traced back to you. The anonymous research data will be retained in our research within our records indefinitely.

Your consent and rights as a Panellist

As a Panellist, participation in this research is voluntary, and you can change your mind at any time. As specified above, when you leave the panel or are removed, we reserve the right to hold your personal data for the sole purpose of preventing any duplicate or fraudulent participation for the duration of the panel, unless you specifically request that we delete all your personal data in accordance with GDPR Article 17 If you:

- Change your mind and no longer wish to participate in this research
- Have any questions or concerns regarding our use of your personal information, our privacy policy or privacy practices.
- Want to request a copy of the personal information we may hold about you, or to request that we correct any inaccurate personal information.
- Want to correct anything inaccurate in your personal data is corrected immediately
- Want to raise an objection, where relevant, about how your personal data is processed
- Request that your personal data is erased if there is no longer a justification for it
- Ask that the processing of your personal data is restricted in certain circumstances

How to contact us

Please contact the panel support team who will assist you. You can contact them via:

Email : panel@ipsosiris.com

Phone : 08000 149464

SMS : 07507303032

To contact us in writing:

Ipsos iris Panel
Ipsos MORI
Kings House
Kymberley Road
Harrow
HA1 1PT

If you have any complaints, we will appreciate if you give us an opportunity to resolve any issue first, by contacting us as set out above. You are, however, always entitled to contact our regulatory body, the UK Information Commissioner at:

https://ico.org.uk/global/contact-us/

Changes to our Privacy Policy

We keep our privacy policy under regular review, and we let you know of any updates. Our privacy policy was last updated on 07/07/2020

Useful links

Ipsos MORI:	www.ipsos-mori.com
Ipsos Group:	www.ipsos.com
UKOM:	www.ukom.uk.net
Information Commissioner's Office:	www.ico.org.uk
World organisation for market research - ESOMAR:	www.esomar.org
Market Research Society:	www.mrs.org.uk

Attachment A - 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 in countries that do not offer an adequate level of protection. 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 Attachment B - Outsourced/Third Party Data Processing apply cumulative.

If Personal Data are transmitted to a recipient outside the Ipsos Group 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 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 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 Subjects 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, the exporting company must document 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 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.

Attachment B - Outsourced/Third Party Data Processing

In many cases Ipsos MORI is using external providers to process Personal Data. In these cases, an agreement on data processing on behalf of Ipsos MORI must be concluded with such provider. This can be done either by way of including appropriate provisions in the agreement governing the overall relationship with the provider or in a separate and specific document. In respect of processing on behalf of Ipsos MORI, the provider may only process the Personal Data as per the 12 instructions from Ipsos MORI. When instructing a provider, the following requirements must be complied with:

- Where the Personal Data in question fall under client data, any relevant client requirements need to be passed down to the provider.
- The provider must be chosen based on its ability to cover the required technical and organisational protective measures and in line with Ipsos MORI supplier approval process
- The provider must not subcontract the processing further without Ipsos MORI'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 MORI and provider must be documented.
- Before the data processing begins, Ipsos MORI must be confident that the provider will comply with its duties. A provider 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 MORI should retain the right to audit the provider's compliance.

- In the event of cross-border contract data processing, the relevant national requirements for disclosing 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 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.
    - Participation of the provider in a certification system accredited by the EU for the provision of a sufficient data protection level.

Attachment C - Privacy by Design and Default

Ipsos MORI 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.