

Privacy statement - Clients

We treat all information that we receive from clients as confidential and do not use the information for any purpose other than to fulfill our obligations to them. We keep client information secure at all times, and prevent the misuse and unauthorised disclosure of it by our employees or any third parties.

Information we collect and store

In order to fulfil our obligations we collect and store the following information:

- Key contact information such as name, company, phone number, job title and department (where relevant).
- Any information provided the client that is of use in carrying out our research objectives on your behalf. This information might contain, but is not limited to:
 - Documents sent when requesting a proposal
 - Email communications.
 - Notes made during telephone communication that are relevant to the project. We never record telephone conversations
 - Supporting documents that have been provided in the course of a project. Such as other relevant research or pertinent information.
- We keep records of any documents generated by ourselves in the course of conducting our research. These include:
 - Reports, summaries and debrief presentations
 - Documents that support the design of the research.
 - Descriptions of analysis procedures used in processing research data.
- Information gathered from participants during the process of our research. For more information please see our [Privacy Statement for Participants](#).

How is this information used?

The information is used to carry out the research objectives we have been commissioned for. In certain instances we will also use the information to approach the client when we believe we have additional services that would be of interest to them.

In certain cases it might also be that new analytical methodologies provide additional insight on historic projects. In this case we might also contact the client to relay the updated findings.

Who we share personal information with

We use third party companies to help administer and run our business. As a result, personal information may be transferred outside of the countries where we and our clients are located. This includes countries outside the European Union and to countries that do not have laws that provide specific protection for personal data. We have taken steps to ensure all personal data is provided with adequate protection.

Companies to which we transfer such information include:

- Google, for the administration and provision of document and email services.
- Hubspot CRM software, for the administration and provision of customer relationship management systems.
- Formentone International, for the purposes of invoicing and accounting.

In addition we may also receive requests from third parties with authority to obtain disclosure of personal data, such as to check that we are complying with applicable law and regulation, to investigate an alleged crime, to establish, exercise or defend legal rights. We will only fulfil requests for personal data where we are permitted to do so in accordance with applicable law or regulation.

Who we share project information with

Client project information is treated as strictly confidential. Information is only ever shared with explicit written permission from the client. Such permission may arise in process of collaboration between multiple agencies on a project.

For certain services it is necessary to transfer assets to additional service providers during the conduct of our research. Companies and information we transfer include:

- Client experiment questionnaires are transferred to third party translation services.
- Client assets (such as images / videos) to be used in the conduct of our research are transferred to Amazon S3 for hosting purposes.

Managing conflicts of interest

We will make every effort to notify our clients of any potential conflicts of interest in the conduct of our research. Only once the client is happy the the conflict is appropriately handled would we proceed with any project.

Rights of access, rectification and erasure

Individuals have certain rights over their personal data and controllers are responsible for fulfilling these rights.

Individuals' rights may include the right of access to personal data, to rectification of personal data, to erasure of personal data / right to be forgotten, to restrict processing of personal data, to object to the processing of personal data, to data portability, the right to withdraw consent at any time (where processing is based on consent) and the right to lodge a complaint with a supervisory authority.

You have the right to obtain confirmation as to whether we process personal data about you, receive a copy of your personal data held by us as a controller and obtain certain other information about how and why we process your personal data (similar to the information provided in this privacy statement)

You have the right to request for your personal data to be amended or rectified where it is inaccurate (for example, if you change your name or address) and to have incomplete personal data completed.

In order to exercise any of these rights please contact us using the link under Queries below.

Security

Mindlab maintains appropriate technical, administrative and physical safeguards to protect information, including, without limitation, personally identifiable information, received or collected by us.

Queries

If you have any queries concerning this policy, our website or our research, please [contact us](#).

This policy was last updated 08/04/19.