Respondent's Privacy Policy

This notice is about how Mindfrog collects, stores, uses and discloses your Personal Data. We are committed to the protection of the confidentiality of Personal Data ("Personal Data") of all of our respondents, following any applicable laws and regulations, and the codes of standards of opinion survey research associations like the Insights Association (www.insightsassociation.org), BHBIA (www.bhbia.org.uk) and EphMRA (www.ephmra.org).

The type of information we collect includes personal data only for research purposes. This includes survey and other research data collected from you; data we may obtain from secondary sources available in the healthcare industry; and any Personal Data you provide. The personal data we collect includes any information relating to an identifiable natural person, who can be identified by reference to an identifier like a name, ID number, online identifier or other factors like the physical, mental, economic, cultural or social identity of that person. For healthcare providers, this includes numbers such as a US ME Number from the AMA.

We never release your Personal Data—we only use it for marketing research and for no other purpose. We do not use the contact information we receive about you for any direct marketing activities, nor do we share your contact information with third-party vendors for the purposes of marketing activities.

We may use your Personal Data include validating answers you provided in a survey; reporting safety issues; ensuring you receive your study honoraria; provide service or support to you as you ask for.

We may use a third-party agent to host our surveys or other research programs or perform other market research-related activities, but our contractual arrangements with these third-party vendors ensure that your personal information will not be shared with anyone and will not be used for any other purpose without your consent.

We may disclose your Personal Data and/or survey responses to third parties as authorized by you or in response to any lawful request by public authorities, to meet national security or law enforcement requirements or pursuant to required legal process; to information technology hosting providers, cloud service providers, market research service providers, our agents, contractors or partners to provide our services.

HEALTHCARE PROFESSIONAL PAYMENT DISCLOSURE REQUIREMENTS
Our payments to healthcare professionals are in accordance with all applicable law and practices. Under these regulations, certain payments to healthcare professionals may be subject to reporting to the respective bodies, who will make the details available for public viewing on its website. If this is required for one of our surveys or research programs, we will advise you as part of the consent process for that specific survey/program. To learn more, please contact us at info@mindfroggroup.com

DISCLOSURE OF SAFETY
Mindfrog is obligated by contractual agreements with our clients to disclose any Adverse Events or Product Quality Complaints that is reported about a medical product. An Adverse Event is something that occurs while a person is on treatment or within a pre-specified time after treatment has been completed. It can include anything from a minor issue (e.g., some minor hair loss) to a more serious change in a person's health (e.g., uncontrolled vomiting). A Product Quality Complaint is any deficiency associated with the product which can include packaging errors, changes in appearance, taste, or smell, and other issues, etc.

If you disclose safety data to us, we will report to the client for whom the research is being conducted only the minimal amount of non-personally identifying information about the affected individual (whether it is you or somebody else) as is needed to satisfy the FDA and other equivalent global regulatory agency requirements. As a reporter of safety data, we may disclose your name and contact information to the client for whom the research is being conducted so that they may follow up with you to obtain additional information that is required only after we have obtained your consent to the disclosure. If you are based in Germany, this is not applicable and only anonymous reports will be submitted to the client.

INFORMATION COLLECTED BY AUTOMATED TECHNOLOGIES
As further specified below, we may automatically collect a variety of machine-readable information about you, including the date and time you visited our website, the pages you visited, the website you came from, the type of browser you are using (e.g., Internet Explorer, Firefox, Safari, Chrome, etc.), the type of operating system you are using (e.g., Windows, mac OS, etc.), your Internet Protocol ("IP")address and the domain name and address of your Internet service provider.

We may also collect the date and time you visited the site; the number of pages you viewed; the time in seconds you spent on each page; and the details of any website you visited before and/or after participation in one of our surveys or other research program.

We do not allow individuals younger than 18 years of age to take part in our research unless verifiable consent for their participation has been given by their parents or legal guardians. Further, we comply with the Children's Online Privacy Protection Act of 1998 ("COPPA").

WHAT SAFEGUARDS ARE THERE TO ENSURE THE SECURITY OF YOUR DATA?
The security of your Personal Data is very important to us. We have put in place reasonable physical, electronic, and administrative procedures to safeguard the information we collect. Only those employees who need access to your information to perform their duties are authorized to have access to your Personal Data. We cannot guarantee that all communications between us or information stored on our servers will be free from unauthorized access by third parties such as hackers, and your use of our services demonstrates your assumption of this risk.

INFORMATION FOR CITIZENS OF THE UK/EU/SWITZERLAND ABOUT CROSS-BORDER TRANSFERS
Mindfrog complies with the Insights Association Data Privacy Framework Services Program as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information from European Union member countries, the United Kingdom and Switzerland. We adhere to the Data Privacy Framework Services Program Principles of Notice, Choice, Accountability for Onward Transfer, Security, Data Integrity and Purpose Limitation, Access, and Recourse, Enforcement and Liability. If there is any conflict between the policies in this privacy notice and the DPF Principles, the DPF Principles shall govern

We may also process Personal Data relating to individuals in the EU, United Kingdom, and Switzerland via other compliance mechanisms, including the consent of such individuals or via data processing agreements based on Standard Contractual Clauses. In compliance with the Insights Association Data Privacy Framework Services Program (EU-U.S. DPF, UK Extension to the EU-U.S. DPF, and Swiss-U.S. DPF), we commit to resolve complaints about your privacy and our collection or use of your personal information (contact info@mindfroggroup.com).

Mindfrog is under the enforcement authority of the U.S. Federal Trade Commission. Under certain limited conditions, individuals may be able to invoke binding arbitration before the Insights Association Data Privacy Framework Services Program Panel to be created by the U.S. Department of Commerce and the European Commission.

Dated October 16, 2025