Privacy Policy

Introduction

Wellside Research Ltd. is a full service independent research consultancy. We undertake social research projects (using both qualitative and quantitative techniques) on behalf of our clients. As such, data forms an integral part of our business and so we take our responsibilities around privacy and data protection very seriously.

We are registered with the Information Commissioners Office (ICO) - reference number: ZA731251.

Our Privacy Policy (as laid out below) details our practices in relation to the collection, processing, storage, retention and sharing of data. Our processes have been reviewed and this policy developed to comply with the GDPR.

Your Rights

The EU General Data Protection Regulation (GDPR) outlines individual's rights as:

- Individuals have the right to be informed about the collection and use of their personal data;
- Individuals have the right to access their personal data;
- Individuals have the right to ask for inaccurate personal data to be rectified, or completed if it is incomplete;
- Individuals have the right to have personal data erased;
- Individuals have the right to request the restriction or suppression of their personal data;
- Individuals have the right to data portability, i.e. this allows individuals to obtain and reuse their personal data for their own purposes across different services;
- Individuals have the right to object to the processing of their personal data in certain circumstances; and
- Rights related to automated decision making including profiling (although, please note that Wellside Research does not undertake automated decision making or profiling).

What Information we Collect

Personal Information Held by Wellside Research:

Personal data is only collected and held by Wellside Research for research purposes, we conduct no marketing or PR activities.

To facilitate research: In order to facilitate our research projects we may collect the names and contact details (such as email addresses, telephone numbers, and/or addresses as well as possibly job titles and the name/nature of the organisation they work for) of individuals to be invited to participate in the research. This information would only be used to make initial contact with possible research participants and invite them to take part. In most situations where this type of data is gathered/held, this either comprises publicly available information (such as professional contact details) or is provided by our clients (where they are authorised to share such information).

When conducting research: Depending upon the nature of the research contract, we may collect personal information during the fieldwork/data collection phase. This could include respondents' gender, age, ethnicity, marital status, employment status, religious beliefs, sexuality, etc, in addition to their views and experiences of the specific research topic. The provision of this information is always optional and never mandatory. Typically, personal information would be provided via questionnaires or during interviews, although a range of data collection methods are used, depending on the nature of the research. At the outset of the work, all potential research participants would be provided with detailed information about the project, the nature of the work and their input, what data will be required and the voluntary nature of all participation/responses, how the data will be used, details of any sharing of the data, etc. This information would also be repeated ahead of any research participation, thus allowing respondents to provide fully informed consent.

How Data is Secured:

All files containing personal or sensitive data are password protected.

Names and contact details are never stored together with research responses. Research responses are either fully anonymised (i.e. so it cannot be linked back to individual respondents) or unique identifiers are used with both files held separately and password protected.

Data files are only accessible to the immediate project team. All team members are required to use password protected computers/laptops.

To facilitate online surveys we use a SmartSurvey account. SmartSurvey fully comply with the GDPR, and provide a detailed privacy policy on their website. Any data provided to us as a result of a research participant responding to one of our online surveys is done so securely. SmartSurvey encrypt all data being entered/transferred. Our account is secured via a password, only known to the account holder. When data (or surveys) are deleted from our SmartSurvey account, these are expunged by SmartSurvey and are no longer stored by them.

Data Sharing:

When data is shared with us (for example from our clients), we would seek to receive data files securely. All such files should be password protected, with the password provided to us under separate coverage to the data files.

Data may also be shared by us with trusted UK based subcontractors from time-to-time, in order to facilitate the research project. This includes other research partners

and/or printing and mailing companies. The data privacy policies and processes of any subcontractor would be scrutinised in advance, and all of our partners would be contracted to adhere to Wellside Research's strict data protection processes. When it is necessary to share data with subcontractors, again password protected files would be used, with the password being provided to the subcontractor under separate coverage to the files.

At the end of research projects, a final data file containing the research results can sometimes be shared with our client, either for ongoing storage or further interrogation. Typically, only anonymised data is shared by us with our clients. All personal data would be removed/edited from any data file before being shared in such a way. Where the client has specifically requested the inclusion of personal/identifiable data within the final data file, research respondents would be made aware of this prior to their participation, and permission sought to share such data with the client. Where permission is not granted, the data gathered would remain anonymous or the participant would opt out of the research. Again, all data files containing sensitive/personal data would be password protected, with the password being communicated to the client separately to the data file.

Data is not transferred internationally.

Cookies:

Wellside Research does not use Cookies within our own website.

Cookies may however, be used to facilitate online surveys. These are used (only where necessary) to ensure that more than one response cannot be submitted by one person or via one device. They may also be used in the event that a survey requires some form of identification of respondents (for example an email address or IP address). Again, we use SmartSurvey to facilitate our online surveys, and more details of their Cookies Policy can be found on their website.

Data Breach

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Should we become aware of any data breach we will alert the relevant authorities as soon as possible.

Where Wellside Research is acting as a data processor for a client, we will alert the client (i.e. the data controller) immediately regarding any type of breach. It is then for the data controller to determine any further action required, such as reporting the breach to the ICO and/or alerting any affected individuals, although Wellside Research will provide all the assistance and support required.

Where Wellside Research is the data controller, we will assess the need for any data breach to be reported to the ICO. Where reporting is required, this will be done as

soon as possible, and always within 72 hours from first detecting a breach. The need for reporting will be determined upon assessing the likelihood and severity of the resulting risk to individual's rights and freedoms, and we will base this assessment on Recital 85 of the GDPR which explains that:

> "A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

Responsibility for managing any data breaches lies with our Director, Elaine Wilson-Smith. We document all breaches, even where these do not need to be reported to the ICO. Any data breach will also result in Wellside Research conducting a full investigation into the source of the breach (i.e. human error or a systemic issue) and the need for corrective measures going forward.

Contacting Us

You can contact us at any time to:

- Request access to the data that Wellside Research has about you;
- Correct any information that Wellside Research has about you;
- Delete any information that Wellside Research has about you.

If you have any additional questions about Wellside Research's collection, processing, storage or retention of data, please contact us at:

Wellside Research, 20 Kerr Loan, Haddington, East Lothian, EH41 3DZ.

Tel. 0131 677 5522

Email. enquiries@wellsideresearch.co.uk