# NWA Data Protection Policy

## NWA Data Protection Policy

### *Introduction*

NWA Social and Market Research Ltd. (NWA) is a Full-Service Market Research Agency founded in 1989. As a Company Partner with the Market Research Society (MRS), NWA abides by the MRS Code of Conduct.

The organisation is committed to being transparent about how it collects and uses the personal data of its Client's service users, members of the public and any others with whom it may come into contact by reason of its professional services; its workforce, and to meeting its data protection obligations. This policy sets out the organisation's commitment to data protection, and individual rights and obligations in relation to personal data.

This policy applies to the personal data of research subjects as a data processor, and business clients, also job applicants, employees, workers, contractors, volunteers, interns, apprentices and former employees, these referred to as HR-related personal data, as a data controller. It also includes client, business contacts and other people the organisation has a relationship with or may need to contact.

The organisation has appointed David Wilburn as its Data Protection Officer (DPO). Their role is to inform and advise the organisation on its data protection obligations. He can be contacted at **david.wilburn@nwaresearch.co.uk** or on 01642 360982. Questions about this policy, or requests for further information, should be directed to the Data Protection Officer.

As a Company Partner the organisation adheres to the Market Research Society (MRS) code of conduct regarding data processing to ensure full compliance with the eight rights of individuals GDPR requirements.

Registration: NWA is registered on the Data Protection Public Register (reference Z1870384).

### *Definitions*

**"Personal data"** is any information that relates to a living individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

**"Special categories of personal data"** means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic and biometric data.

**"Criminal records data"** means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

### *Data protection principles*

The organisation processes personal data in accordance with the following data protection principles:

- The organisation processes personal data lawfully, fairly and in a transparent manner.
- The organisation collects personal data only for specified, explicit and legitimate purposes.
- The organisation processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- The organisation keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- The organisation keeps personal data only for the period necessary for processing.
- The organisation adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

The organisation informs individuals of the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons. If the organisation wants to start processing data for other reasons, individuals will be informed of this before any processing begins.

Data will not be shared with third parties, except as set out in privacy notices. Where the organisation relies on its legitimate interests as the basis for processing data, it will carry out an assessment to ensure that those interests are not overridden by the rights and freedoms of individuals.

Where the organisation processes, special categories of personal data, or criminal records data to perform obligations, to exercise rights in employment law, or for reasons of substantial public interest, this is done in accordance with legislation.

The organisation will update personal data promptly if an individual advises that their information has changed or is inaccurate.

Personal data gathered during the employment, worker, contractor or volunteer relationship, or apprenticeship or internship is held in the individual's personnel file (in hard copy or electronic format, or both), on HR systems, in Cloud based storage and the computerised office system. Employee paper files are kept in a locked filling cabinet within the office at all times. The periods for which the organisation holds HR-related personal data is 6 years after termination.

The organisation keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

### *Client Data*

Data gathered on behalf of a client, is destroyed as soon as possible after the contract is completed (no later than a 3-month period). Paper questionnaires are certified as confidentially shredded by a contractor, files are electronically shredded, and any digital recordings are erased.

### *Data Protection Risks*

This policy helps to protect the organisation from some very real data security risks, including:

- breach of confidentiality and public trust; for instance, information being shared inappropriately;
- failing to offer choice; for instance, all individuals should be free to choose how the organisation uses data relating to them when the processing is by consent;
- failing to observe the enhanced rights that citizens have under the GDPR - for example, right of access, right to rectification, etc;
- reputational damage; for instance, NWA could suffer if hackers were to successfully corrupt, gain access to or steal sensitive data.

### *Our Roles and Responsibilities*

Our responsibilities are:

- NWA is the data controller under Data Protection Legislation for the personal data it processes for its own purposes. It is also a data processor for client data.
- the Data Protection Officer (DPO) is responsible for monitoring progress and advising the organisation on implementation of this policy; acting as primary contact on any data protection queries; and approving responses to Right of Access requests

(generally described in this document as 'Subject Access Requests');

- the DPO is also responsible for monitoring the completion of all mandatory training for all employees (with special emphasis on employees handling personal data on daily basis) and to ensure access to further guidance and support;
- the DPO will conduct regular assurance activity to monitor and assess new processing of personal data;
- the DPO will monitor and report on all data processor requirements e.g. Roles & Responsibilities, notification, data subject access requests;
- the DPO is the first point of contact for the regulatory authorities and for individuals whose data is processed (employees, customers etc.).

### *Individual rights*

As a data subject, individuals have a number of rights in relation to their personal data.

### *Subject access requests*

Individuals have the right to make a subject access request. If an individual makes a subject access request, the organisation will tell them:

- whether or not their data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- to whom their data is or may be disclosed, including to recipients located outside the UK and the safeguards that apply to such transfers;
- for how long their personal data is stored (or how that period is decided);
- their rights to rectification or erasure of data, or to restrict or object to processing;
- their right to complain to the Information Commissioner if they think the organisation has failed to comply with their data protection rights; and
- whether or not the organisation carries out automated decision-making and the logic involved in any such decision-making.

The organisation will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless they agree otherwise.

If the individual wants additional copies, the organisation will charge a fee, which will be based on the administrative cost to the organisation of providing the additional copies.

To make a subject access request, the individual should send the request to the Data Protection Officer **david.wilburn@nwaresearch.co.uk**. In some cases, the organisation may need to ask for proof of identification before the request can be processed. The organisation will inform the individual if it needs to verify their identity and the documents it requires.

The organisation will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the request is complex, it may respond within three months of the date the request is received. The organisation will write to the individual within one month of receiving the original request to tell them if this is the case.

If a subject access request is manifestly unfounded or excessive, the organisation is not obliged to comply with it. Alternatively, the organisation can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded if it is made with the intention of harassing the organisation or causing disruption, or excessive where it repeats a request to which the organisation has already responded. If an individual submits a request that is unfounded or excessive, the organisation will notify them that this is the case and whether or not it will respond to it.

### *Other rights*

Individuals have a number of other rights in relation to their personal data. They can require the organisation to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override the organisation's legitimate grounds for processing data (where the organisation relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the organisation's legitimate grounds for processing data.

To ask the organisation to take any of these steps, the individual should send the request to the Data Protection Officer **david.wilburn@nwaresearch.co.uk**

### *Data security*

The organisation takes the security of all personal data seriously. The organisation has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

Where the organisation engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

### *Impact assessments*

Some of the processing that the organisation carries out may result in risks to privacy. Where processing would result in a high risk to individual rights and freedoms, the organisation will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

### *Data breaches*

If the organisation discovers that there has been a breach of any personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner and, as appropriate with the client, within 24 hours of discovery. The organisation will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

If the breach in relation to a client of the organisation the Data Protection Officer will notify the clients Data Protection Officer immediately, along with the ICO and provide the client with information about its likely consequences and the mitigation measures it has taken.

### *International data transfers*

The organisation will not transfer HR-related personal data to countries outside the UK.

### *Individual responsibilities*

Individuals are responsible for helping the organisation keep their personal data up to date. Individuals should let the organisation know if data provided to the organisation changes, for example if an individual moves to a new house or changes bank details.

Individuals may have access to the personal data of other individuals and of our customers and clients in the course of their employment, contract, volunteer period, internship or apprenticeship. Where this is the case, the organisation relies on individuals to help meet its data protection obligations to employees and to customers and clients.

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction as set out below in this policy);
- not to remove personal data, or devices containing or that can be used to access personal data, from the organisation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;
- not to store personal data on local drives or on personal devices that are used for work purposes; and
- to report data breaches of which they become aware to David Wilburn the Data Protection Officer immediately.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the organisation's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

### *Data Storage*

When data is stored on paper, it is kept in a secure place where unauthorised people cannot see/access it. When not required, sensitive paper files are kept in a locked drawer or filing cabinet;

Employees are instructed to make sure sensitive paper and printouts are not left where unauthorised people could see them and are shredded confidentially when no longer required.

Data stored electronically is protected from unauthorised access, accidental deletion and malicious hacking attempts: using strong passwords that are changed regularly and never shared.

Data is stored on designated drives and servers and will only be uploaded to safety secured cloud computing service.

Data is backed up every four hours and regularly tested.

### *Data Use*

When working with personal data, employees will ensure their computers are always locked when left unattended.

Personal data is encrypted before being transferred electronically outside of the organisation's domains.

### *Data Accuracy*

The law requires the organisation to take reasonable steps to ensure data is kept accurate and up to date. It is incumbent upon the organisation to ensure personal data held and processed is accurate and to ensure it continues to be accurate. It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

Employees are expected to take every opportunity to ensure data is updated. For instance, by confirming a client or respondent's details when they call. The organisation will make it easy for data subjects to update the information the organisation holds about them.

Data is updated as inaccuracies are discovered. For instance, if a respondent can no longer be reached on their stored telephone number, it is removed from the database and the client informed.

### *Consent - Respondents to Surveys, Focus Groups, etc.*

We use appropriate wording to ensure clear affirmative action by respondents. We ensure that we have full consent freely given, specific, informed and unambiguous. This includes the provision of information on the collection and retention of their data. All respondents are made aware that they have the right to withdraw their consent and are informed of this prior to giving their consent. We ensure that we have full consent of respondents freely given, specific, informed and unambiguous. This includes the provision of information on the collection and retention of their data. All respondents are made aware that they have the right to withdraw their consent and are informed of this prior to giving their consent.

In line with recommendations from our professional body (MRS) we believe that the most effective approach in delivering the extensive information required under GDPR is to provide this in 'layers', allowing individuals to immediately receive essential information and to access more detailed information as required.

### *Training*

The organisation provides training to all individuals about their data protection responsibilities upon commencement of employment and annually thereafter. To this end NWA has entered into a contractual relationship with a supplier of online training for all staff on their roles and responsibilities in relation to Data Protection/GDPR. The training company is responsible for ensuring the training is up to date and compliant with current legislation. This training is mandatory for all staff and certificates of successful completion are kept on employee records.

Individuals whose roles are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.