UK General Data Protection Regulation (UK GDPR) Policy

PFA Research Ltd

May 2022

Contents

1 Policy Statement

This document outlines how PFA Research complies with the UK General Data Protections Regulation (UK GDPR) when conducting market and social research as well as conducting its business. UK GDPR sets out seven key principles when collecting, processing and holding data, namely:

1. Lawfulness, fairness and transparency – Data must be processed lawfully, fairly and in a transparent manner.
    a. Lawfulness can include: user consent; contractual obligations; legal obligations; protection of vital interests of a natural person' public task; legitimate interest (but not overriding data subject's rights and interests)
    b. Fairness means data should not be collected or processed by purposely withhold information about what or why data is collected. Furthermore, data won't be mishandled or misused.
    c. Transparency means when collecting and/or processing data the data controller or data processor has to be clean, open and honest with the data subjects about who, why and how the data is collected and/or processed.
2. Purpose Limitation - Collected for the specified, explicit and legitimate purposes and not further processed incompatibly. Further processing for research is explicitly compatible.
3. Data Minimisation– Adequate, relevant and limited to what is necessary in relation to purposes for which processed.
4. Accuracy – Accurate and kept up to date.
5. Storage limitation – The length of time data is stored must be justifiable.
6. Integrity and confidentiality (security) – Data must be protected from unauthorized or unlawful processing and accidental loss, destruction or damage.
7. Accountability – Appropriate measures and records must be in place as proof of compliance with the data processing principles.

Under the UK GDPR, an individual or company can be:

- A Data Controller – whereby the company determines the purpose and manner in which data is to be collected and used;
- A Joint Data Controller – whereby the company jointly determines with another party the purposes and manner in which data is collected and used;
- A Data Processor – whereby the data is processed on behalf of a controller.

PFA Research Ltd may be required to fulfil one or more of the above roles. This is discussed further below.

This policy will mention the following: Data subjects, personal data, data controllers and data processors. Where these are mentioned, the terms are defined as:

Data Subject: a natural person whose personal data is processed by a data controller or data processor.

Personal data: any information related to a natural person or 'Data Subject' that can be used to directly or indirectly identify the person.

Data controller: the entity that determines the purpose, conditions and means of the processing of personal data.

Data processor: the entity that processes data on behalf of the Data Controller.

In accordance with advice given by the Market Research Society (https://www.mrs.org.uk/) PFA Research has voluntarily appointed a Data Protection Officer (DPO). If you have need to contact the DPO for PFA Research please email dpo@pfa-research.com or call +44 (0) 1326 3765705 and ask for the Data Protection Officer.

2 Data subjects rights

2.1 Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.

When collecting, processing and holding personal data, PFA Research will always identify the lawful basis for processing the data.

Where data is collected by PFA Research, either as data controller or data processor, PFA Research will ensure that data is always collected and processed with informed consent of the individual, that data is processed lawfully and fairly and in a transparent manner.

In detail, PFA Research will ensure that individuals are fully informed as to how their data will be used prior to providing data in order to give informed consent. Individuals' consent will be collected using positive action, e.g. by verbal response, opt-in sign up or written response.

Data is not processed in any way which is incompatible with the information given when the data subject gave their informed consent. Where we ask data subjects for sensitive data – defined by the UK GDPR as race, ethnic, origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sexual orientation or sex life – PFA's condition for processing sensitive data is the data subject giving explicit informed consent to the processing of those personal data for one or more specified purposes. We will only collect this type of data where necessary and data impact assessments will be established to ensure the purpose of the collection. Data subjects will be given the option to not answer any question they do not wish to answer in accordance with the Market Research Society Code of Conduct.

Where personal data has been shared with PFA Research by a third party, making PFA Research the data processor, we will ensure that there is a lawful basis for processing such data. Lawful basis is most likely to be 'legitimate interest' by the data controller to have the data subject take part in market or social research in order to inform their business/organisation purpose by understanding more about their customers/clients or potential customers/clients and therefore being able to improve products/services.

PFA Research will be transparent in their collections, processing and holding of personal data. During any research (or on request) data subjects are informed on the following:

- Informed about who PFA Research are, how they can be contacted;
- Why personal data is collected as part of research and sponsor and/or objective of the research undertaken;
- How the data subjects' personal or sensitive personal data will be used.

PFA Research will not keep personal data for longer than is necessary and only for the purpose which the data was collected for. As a minimum PFA Research will review whether it is necessary to keep any personal data for a period of time (e.g. 12 months) after the data is collected and delete any personal data which is not necessary to keep. An expiry and destroy date is always logged for any retained personal data.

PFA Research will not share any personal data with third parties without prior and explicit consent from the data subject unless under legal obligation to do so.

Data subjects have the right to lodge a complaint with the data controller using PFA Research' contact details, of if they are still not satisfied, the Information Commissioners Office should they wish, using the helpline 0303 123 1113. All contact details are published on the PFA Research web site.

2.2 The right of access

Data subjects have the right to request access to any information which PFA Research hold about them if it is linked to their personal data in anyway. If PFA Research receives such a request of access to data, it is PFA's policy to record the request, respond with an acknowledgement within 48 hours and provide the data to the individual within 30 days from the date of the initial request in accordance with UK GDPR guidelines. If data which is held is no longer personally identifiable in any way, the data subject is informed thus.

2.3 The right to rectification

Data subjects have the right for their data to be rectified if they believe it is inaccurate or incomplete. If PFA Research receives a request to rectify personal data from an individual which we hold data about, it is our policy to record the request, respond to that request within 48 hours in acknowledgement and within 30 days will make the rectification or completion as requested following UK GDPR guidelines.

2.4 The right to erasure, the right to object and the right to restrict processing

Data subjects have the right to object to the processing of their data and withdraw consent to their data being processed at any point. This can include asking PFA Research to erase any personal data which we hold, restrict processing of that personal data or object to a type of processing which PFA Research is undertaking. Data subjects are given information of how to withdraw their consent or request restricted processing or erasure. All information on contacting PFA Research for this purpose are also published on the PFA Research web site.

PFA Research will record any request for erasure, objection or restricted processing and respond within 48 hours in acknowledgement and within two weeks to carry out the request.

2.5 Personal data shall be collected for specified, explicit and legitimate purposes and not further processes in a manner that is incompatible with those purposes.

PFA Research will always specify in an explicit and transparent manner the reason data subjects' personal or personally sensitive data is being processed. Any data is not processed further in any way which is incompatible with those purposes without the explicit informed consent of the data subject.

PFA Research will ensure that data sharing agreements are in place for any personal data shared with PFA Research by data controllers (e.g. our clients) or for any personal data shared by PFA Research with data processors. This will ensure that a legitimate purpose is established.

2.6 Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed.

PFA Research will only collect data which is necessary for individual and specific projects or lawful or legitimate purposes, either as part of our work for our clients or as part of running our business.

Where we collect sensitive data, data subjects are told why it is necessary to collect this data and given the option to answer or not to answer the request.

Personal data is not kept for longer than necessary and data is anonymised and/or securely deleted at the earliest possible point (see section 2.1.)

2.7 Personal data shall be accurate and, where necessary, kept up to date: every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purpose for which they are processes, are erased or rectified without delay.

All data subjects are informed that they have the right to their data being rectified if they believe it to be inaccurate or incomplete. If we receive a request to rectify personal data, it is PFA Research's policy to respond to that request within 48 hours in acknowledgement and the rectifications to be made within 30 days of the initial request received. Information on how to contact PFA Research is given to data subjects directly and can also be found on our web site.

2.8 Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

PFA Research does not keep personal data longer than is necessary and will anonymise data or delete personal data at the earliest possible point, unless instructed differently by third party clients, data subjects or law enforcement. All collected personal data should be reviewed at least 12 months after collection and necessity of further storage or secure deletion assessed at this point.

2.9 Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

PFA Research uses a selection of IT equipment, software and applications to undertake its work, including processing of data, personal data and sensitive personal data. To ensure that the data processing is secure and personal data is protected against unauthorised or unlawful processing and/or against accidental loss, destruction or damage, we will only work with suppliers which demonstrate full compliance with UK GDPR. We will be happy to provide further and in-depth details on all of them if necessary.

For our in-house IT requirements we work with local company Piran Technologies (https://pirantech.co.uk/) based in Redruth Cornwall, who ensure that our IT equipment and software applications are up-to-date on security and protection against malware and other malicious software.

For online data collections we primarily use UK based Snap Surveys (www.snapsurveys.com), who are independently audited and certified by Bureau Veritas as being compliant with ISO 27001 Information Security Systems, and Survey Anyplace (www.surveyanyplace.com) who,

based in Belgium, fully comply with the GDPR. For telephone interviews we primarily use Nebu BV, based in the Netherlands, ISO 27001 and ISO9001 certified and compliant with GDPR. We will occasionally use other online data collection providers who will be assessed accordingly for full compliance with the UK GDPR.

All transfer of personal and personally sensitive data is conducted via a dedicated site on PFA Research dedicated and licenses Microsoft SharePoint application (MS365) in order to protect the data at their most vulnerable – during transfer. Sensitive personal data will additionally be password protected during transfer if necessary.

PFA Research takes cyber security very seriously, and as this policy outlines our commitment and compliance with the UK GDPR, PFA Research has furthermore an IT Security policy. Our IT Security Policy regulates employees' access to data, other password protection and security measure in more detail.

3 Transferring of personal data

PFA Research will use a dedicated 'dropbox' site within its own Microsoft Sharepoint domain for transfer of all personal data. We ask all third parties who transfer data to PFA Research to use the same or similar secure software/portals (such as Egress Switch) when transferring personal data to PFA Research.

For any personal data shared, a data sharing agreement is put in place and signed. PFA Research will issue data sharing agreements if the data controller and can provide a template for data controllers if PFA Research acts as the data processor.

PFA Research will not share personal data with any unauthorised third party and undertakes relevant checks to ensure that any third party with whom data is shared on request of clients or data subjects, comply with the UK GDPR. The only exceptions are as outlined in the UK GDPR for compliance with legal obligations.

4 The Use of Data Protection Impact Assessments (DPIA)

A DPIA will be required if projects or procedures are initiated which may impact upon the rights of data subjects. Examples may include (but are not limited to):

- Large scale processing of special category data
- The proposed implementation of new software (such as a new CATI system)
- Large scale processing/profiling of children
- Introduction of technologies (such as the capture of tracking data)
- Requirements to match or combine data from different data sources

All core staff will be made aware of the requirement for a DPIA and may request one at any time.

The DPIA will be fully documented using the DPIA template (see separate document).

5 Informed consent

Under UK GDPR PFA Research has a lawful basis for processing personal data under the grounds of consent. The consent of respondents is two-fold:

- Firstly, they must have consented to have their personal details used for market research purposes (either on the basis of their contract with the client providing the

data) or, in the case of purchased sample, have given their consent to a third party to use their data for market research purposes
- Secondly, at the time of contacting the respondent, they must be given the opportunity to provide their informed consent to participate in the research study

5.1 Informed consent for primary market research (data collection)

During any primary research (data collection) project, PFA Research requires participants to consent to taking part. Consent to participate by respondents must be:

- Freely given
- Specific
- Informed
- Unambiguous

Consent to telephone surveys:

- The interviewer must provide the respondent with all relevant details in order for them to provide their informed consent
- A record must be kept of this consent either by:
    - An audio recording of the consent (provided that the respondent has already agreed to audio recording); and/or
    - A contemporaneous note of the respondent's consent recorded in the survey script
- The approach to obtaining informed consent can by 'layered' in the sense that it is not practical to provide a respondent with all of the required information in the first few seconds of a telephone call
- However, at the first layer, i.e. as part of the survey introduction, we need to say:
    - Who we are
    - Who we are calling on behalf of
    - The purpose of the call
    - The amount of time required for participation
    - The fact that all of their information will be treated anonymously and in confidence or an explanation to different circumstances
    - Assurance that the survey is being conducted in accordance with the Market Research Society Code of Conduct
    - That the respondent has the right to withdraw their consent to participate at any time
    - Obtain consent to record the call
- At the second layer, i.e. at the end of the survey, the respondent should be:
    - Offered the MRS Freephone number
    - Offered the PFA Research phone number
    - Offered the PFA Research website address where full contact details and the data privacy policy can be found
    - A reminder that they can recontact us to withdraw their consent to participate after reviewing the policy

Consent to online surveys:

- The principles are the same as for telephone interviews
- However, consent can be given by an appropriately worded introduction and asking the respondent to click a box to give a positive opt-in if deemed necessary. Alternatively, an instruction can be included to state that by clicking 'Next' the respondent is happy to participate in the research.

- Prior to the opt-in a link can be provided to our website and specific reference made to the privacy policy

6 Staff training

PFA Research is committed to ensuring that all staff are familiar with their responsibilities under UK GDPR and the Data Protection Act 2018 and will provide training accordingly. Training will be organised as follows:

- As part of their induction, staff will be provided with a detailed introduction to the requirements of the UK GDPR.
- Training will be refreshed if and when necessary, and with updates at least annually.
- Ad hoc training will be carried out as and when needed or if and when new legislative requirements come into force or when a new internal procedure is introduced.

The training will cover:

- Overview of UK GDPR and the core principles as well as an overview of the Data Protection Act 2018.
- Online, certified UK "GDPR Essentials" training course.
- Detailed coverage of relevant processes and procedures for handling personal data (including data provided or collected during the course of market research studies and the use of personal data relating to employees).
- Familiarity with all relevant company policies.

All training will be documented and staff will be required to sign to confirm that they have received the appropriate training.

7 Policy Compliance

This policy is part of the PFA Research employee handbook and staff are made aware of this policy. Complying with the policy and the associated procedures is a key requirement. The policy is also published on the PFA Research website (www.pfa-research.com/gdpr).

Staff are encouraged to feedback any suggestions or concerns they have on any or all aspects of compliance, this or other policies or procedures.

If any party is found to have breached this policy, they may be subject to PFA Research's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager, the data protection officer or managing director.

Likewise, any questions and enquiries in relation to this policy and the associated procedures should be addressed to the line manager, data protection officer and/or managing director.

8 References

The following PFA Research Ltd policy documents and procedures are directly relevant to this policy, and are referenced within this document:

- Data Protection Policy
- Information Security Policy
- Email and Internet Policy
- Business Continuity Management Plan
- Emergency Response Plan
- Procedures for processing and handling samples containing personal data

9 Authorisation, Approval and Review Dates

This Policy will be subject to review annually. This review will not preclude any amends to this or other policies in the interim, should they be deemed necessary or required by law.

10 Alternative Formats

PFA Research Ltd. would like to ensure that your needs are met. If you need this information in any other format or translated into a language other than English, please contact:

PFA Research Ltd
Tremough Innovation Centre
Penryn
Cornwall
TR10 9TA
Tel: 01326 375705
info@pfa-research.com
www.pfa-research.com

11 Version History

Reviewed	Next Review	Reviewed by
May 2018	April 2019	Beate Galke – DPO
April 2019	April 2020	Beate Galke – DPO
August 2020	August 2021	Beate Galke – DPO
October 2021	October 2022	Beate Galke – DPO
May 2022	May 2023	Beate Galke – DPO Review following change over to MS365