UK General Data Protection Regulation (UK GDPR) Policy

PFA Research Ltd

Contents

1 Policy Statement

PFA Research Ltd ("PFA Research") is committed to protecting the rights and freedoms of individuals whose personal data we process. We conduct market and social research in accordance with:

- the UK General Data Protection Regulation (UK GDPR)
- the Data Protection Act 2018
- where applicable, the EU GDPR
- applicable guidance issued by the Information Commissioner's Office (ICO)

We apply data protection by design and by default and maintain appropriate technical and organisational measures to demonstrate accountability.

PFA Research is committed not only to complying with data protection legislation but to being able to demonstrate that compliance at all times. Evidence of compliance is maintained through documented procedures, audit trails, and governance oversight.

This policy explains how PFA Research meets its obligations when acting as a **controller**, **joint controller**, or **processor**.

Separate policies exist for:

- Information Security
- Data Protection procedures
- Data Retention
- External Privacy Notices
- AI governance

2 Scope

This policy applies to:

- all employees
- contractors and temporary staff
- any third party processing personal data on behalf of PFA Research

3 Definitions

Personal data – any information relating to an identified or identifiable natural person.

Special category data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for identification, health data, or data concerning sex life or sexual orientation.

Controller – determines the purposes and means of processing.

Processor – processes personal data on behalf of a controller.

Data subject – the individual to whom the data relates.

4 Data Protection Principles

PFA Research processes personal data in accordance with the principles of:

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality
7. Accountability

5 Lawful Basis for Processing

PFA Research identifies and documents an appropriate lawful basis before processing begins.

Depending on the activity, processing may rely upon:

- consent
- legitimate interests
- contractual necessity
- legal obligation
- public task

Where **special category data** is processed, an additional condition under Article 9 will be met, typically:

- explicit consent, or
- research/statistical purposes with appropriate safeguards under the Data Protection Act 2018.

Other conditions under Schedule 1 of the Data Protection Act 2018 may apply where relevant.

Where legitimate interests are relied upon, a **Legitimate Interest Assessment (LIA)** will be conducted.

Ethical consent required by professional standards (e.g., MRS Code of Conduct) may be obtained even where GDPR lawful basis is not consent.

PFA Research maintains documented internal records mapping common processing activities to the applicable lawful bases and, where relevant, Article 9 conditions and

Schedule 1 DPA 2018 provisions. These are reviewed periodically and when new processing activities are introduced.

6 Children and vulnerable data subjects

Where projects involve children or individuals who may be vulnerable, PFA Research applies enhanced safeguards. These include age-appropriate privacy information, assessment of capacity to consent, involvement of guardians where required, and additional security and minimisation measures.

7 Roles and Responsibilities

When acting as Controller

PFA Research is responsible for:

- determining lawful basis
- providing transparency information
- enabling data subject rights
- ensuring appropriate safeguards

When acting as Processor

PFA Research will:

- act only on documented instructions
- maintain confidentiality
- implement security measures
- assist the controller with rights requests and breaches
- delete or return data at contract end
- permit audits where required

Senior management holds ultimate responsibility for ensuring adequate resources, oversight and a culture of compliance. Data protection risks and incidents are reported to senior leadership on a periodic basis.

Joint Controllers

Respective responsibilities will be defined in an arrangement between parties.

8 Transparency

Individuals will be provided with privacy information in line with Articles 13 or 14, typically via project materials or privacy notices. This includes information about:

- identity and contact details
- purposes of processing

- lawful basis
- recipients
- international transfers
- retention
- rights
- complaint routes

Where data is obtained indirectly, PFA Research will provide Article 14 information within the statutory timeframe unless a lawful exemption applies. Decisions to rely on exemptions are documented.

9 Data Subject Rights

Subject to legal limitations, individuals may have rights to:

- access
- rectification
- erasure
- restriction
- objection
- data portability
- rights related to automated decision-making and profiling

Requests will be logged and responded to within **one month**, with extensions applied where legally permitted.

Where data has been anonymised such that identification is no longer possible, rights may not apply.

PFA Research may request reasonable information to verify identity before fulfilling a request.
Requests may be refused or a reasonable fee charged where they are manifestly unfounded or excessive.
Where research exemptions under the DPA 2018 are applied, the rationale will be documented and approved through the compliance framework.

10 Research Provision and Safeguards

Where personal data is processed for research or statistical purposes, PFA Research applies safeguards such as data minimisation and pseudonymisation.

In accordance with Article 89 UK GDPR and the Data Protection Act 2018, certain rights may be restricted where their exercise would seriously impair research outcomes and where appropriate protections are in place.

Technical and organisational measures supporting these safeguards include pseudonymisation, controlled access to identifiers, aggregation of outputs, and ethical review processes.

Further processing for research purposes is assessed for compatibility in accordance with Article 5(1)(b) UK GDPR.

11 Data Minimisation and Purpose Limitation

Only data necessary for defined research or business purposes will be collected and processed. Data will not be reused for incompatible purposes.

12 Accuracy

Reasonable steps are taken to ensure data is accurate. Mechanisms exist for individuals to request corrections.

13 Retention

Personal data is retained only as long as necessary and in accordance with the PFA Research **Data Retention Policy**, contractual obligations and legal requirements.

Data will be securely deleted or anonymised when no longer required.

14 Security of Processing

PFA Research implements appropriate technical and organisational security measures. Further detail is contained within the Information Security Policy.

Measures include, as appropriate:

- access controls
- encryption and secure transfer
- supplier assurance
- confidentiality obligations
- resilience and recovery capability

Security measures are selected following assessment of the likelihood and severity of risks to individuals and are reviewed periodically.

15 International Transfers

Where personal data is transferred outside the UK, PFA Research ensures that a valid UK transfer mechanism is implemented, including adequacy regulations, the UK International Data Transfer Agreement (IDTA) or the UK Addendum to EU Standard Contractual Clauses, alongside risk assessments where required, such as:

- adequacy regulations
- International Data Transfer Agreements (IDTA)
- Standard Contractual Clauses
- other legally recognised safeguards

16 Data Processing and Sharing

Data sharing with clients, partners or suppliers will occur only where:

- there is a lawful basis, and
- appropriate contractual protections are in place.

Processors and sub-processors are subject to proportionate due diligence prior to appointment and ongoing monitoring thereafter.

17 Data Protection Impact Assessments (DPIAs)

DPIAs are conducted where processing is likely to result in high risk to individuals, including examples such as:

- large scale special category processing
- new technologies
- profiling vulnerable groups
- data matching

DPIAs are documented and maintained within the compliance framework. DPIAs must be completed and approved before high-risk processing begins. Outcomes are tracked and mitigating actions monitored.

18 Automated decision-making

PFA Research does not carry out automated decision-making that produces legal or similarly significant effects on individuals. Where profiling is used for research methodology, it does not impact individuals in this way.

19 Personal Data Breaches

All suspected or actual breaches must be reported immediately in line with internal procedures.

Where required, PFA Research will notify:

- the ICO within 72 hours, and
- affected individuals where high risk is identified.

All incidents, whether notifiable or not, are recorded with rationale for decisions taken.

20 Accountability and Governance

PFA Research maintains evidence of compliance, including:

- records of processing activities
- DPIAs
- LIAs
- staff training records
- processor agreements
- security controls

Privacy by design and default is embedded into project lifecycles through measures such as collection of the minimum necessary data, separation of contact details from research responses, role-based access controls, early anonymisation, and secure disposal.

Compliance documentation is made available to regulators and clients where appropriate. Internal audits or reviews may be conducted to test effectiveness.

21 Training

Additional role-specific training is provided where staff handle higher-risk or special category data. Completion is documented.

22 Complaints

Individuals may raise concerns with PFA Research via the Data Protection Officer. They also have the right to complain to the ICO (www.ico.org.uk, helpline: 0303 123 1113).

23 Data Protection Officer

PFA Research has appointed a Data Protection Officer.

Email: dpo@pfa-research.com
Telephone: +44 (0)1326 375705

Address: Tremough Innovation Centre, Penryn, TR10 9TA

The DPO operates independently and reports to senior management. The DPO is involved in a timely manner in matters relating to personal data and is provided with necessary resources to perform their tasks.

24 Compliance

Failure to comply with this policy may result in disciplinary action and, where appropriate, legal proceedings.

25 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.

26 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

27 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
May 2023	May2024	Beate Galke – DPO
May 2024	May 2025	Beate Galke – DPO
May 2025	May 2026	Beate Galke – DPO
February 2026	February 2027	Beate Galke – DPO