Data Protection Policy Statement

PFA Research Ltd

Contents

1 Data Protection Policy Statement 2

1.1 Purpose and aim of policy 2

1.2 Policy Statement 2

1.3 Responsibilities 2

1.4 Procedures and Guidelines 3

1.5 Data Security Statement 3

2 Procedures in the event of security breach 3

2.1 Containment and recovery 4

2.2 Assessing the risk 4

2.3 Notification of breaches 5

2.4 Review and Evaluation 6

3 Compliance 6

4 References 7

5 Authorisation, Approval and Review Dates 7

6 Alternative Formats 7

7 Version History 8

1 Data Protection Policy Statement

1.1 Purpose and aim of policy

To ensure that PFA Research Ltd (PFA Research) applies appropriate measures to comply with the provisions of the Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR), to meet its statutory obligations and mitigate against penalties under the Act and/or regulation.

PFA Research will carry out its operations so as to adhere with the seven data protection principles, as follows:

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 and/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 handler and/or data processor has to be clear, 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.

1.2 Policy Statement

PFA Research regards the lawful and correct treatment of personal information as imperative to the success of its business and to maintaining the confidence of those with whom we deal. PFA Research will always do its utmost to ensure that we treat personal information lawfully and correctly. To this end we fully endorse and adhere to the Principles of Data Protection as outlined in the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR).

1.3 Responsibilities

All employees are responsible for safeguarding data as outlined in this policy. Data Protection training will be provided to all staff, refreshed annually and supplementary procedures for data processing and database management are also available.

Overall responsibility for the policy's implementation lies with the Managing Director.

1.4 Procedures and Guidelines

PFA Research adheres to the Market Research Society Code of Conduct and guidelines set out by it. The data protection guidelines can be found at https://www.mrs.org.uk/code

Client projects will have specific security guidelines if deemed necessary (i.e. work with vulnerable groups, etc.)

Staff will be briefed at the commencement of each project and provided with any specific guidelines and training with regards to data protection and confidentiality.

PFA Research also operates a 'clear desk' policy and all data processing material should be returned to one central safe place at the end of each working day in order to counteract the possibility of data being compromised.

All printed material deemed confidential and/or sensitive in nature should be disposed of in secure waste disposal, through cross shredding before being disposed (for small amounts of paper) or being destroyed on site through secure means (for large amount of paper).

Procedures are in place to ensure that electronic files are deleted from equipment used during field research and remote working once the data has been transferred and is stored securely within the PFA Research system.

1.5 Data Security Statement

PFA Research has taken measures to guard against unauthorised or unlawful processing of personal data and against accidental loss, destruction or damage.

This includes, but is not limited to:

- Adopting an information Security Policy
- Maintaining a standard operating procedure for data processing
- Taking steps to control physical security
- Putting in place controls on access to information (limitation of access on a 'need to know basis', additional password protection on files if needed, deactivation of user accounts when employees leave PFA Research, etc.)
- Establishing a business continuity/disaster recovery plan
- Training all staff on security systems and procedures
- Detecting and investigating breaches of security should they occur (in accordance with the data breach procedures outlined in Section 2 below)
- Data backups to mitigate accidental loss, destruction or damage.

2 Procedures in the event of security breach

This section sets out the points that need to be considered in the event of a security breach. The guidelines and procedures here listed have been aligned with the Information Commissioners Office published guidelines on data security breach.

As an organisation which processes personal data we must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data.

A data security breach can happen for a number of reasons:

- Loss or theft of data equipment on which data is stored
- Inappropriate access controls allowing unauthorised use

- Equipment failure
- Human error
- Unforeseen circumstances such as fire or flood
- Hacking attack
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it.

However the breach has occurred, there are four important elements to any breach management plan:

1. Containment and recovery
2. Assessment of ongoing risk
3. Notification of breach
4. Evaluation and response

2.1 Containment and recovery

Data security breaches will require not just an initial response to investigate and contain the situation, but also a recovery plan including, where necessary, damage limitation. This will often involve input from specialists across the business such as IT, HR and legal and in some cases contact with external stakeholders and suppliers. In the event of a data security breach should be observed:

- The Data Protection Officer and the Managing Director are informed of the data breach at the earliest possible opportunity following the discovery of a data breach.
- The Managing Director, supported by the Data Protection Officer, will take the lead on investigating the breach and ensure that appropriate resources are in place.
- Establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. This can be, but not being limited to, isolating or closing a compromised section of the network, finding a lost piece of equipment or similar.
- Establish whether there is anything that can be done to recover any losses and limit the damage the breach has caused. As well as the physical recovery of equipment, this can involve the use of back-up tapes to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts.
- Where appropriate, inform the police and/or other relevant authorities, such as the Information Commissioner's Office.

A clear and true record should be made of the nature of the breach, the investigation and the actions taken to mitigate it. This record should include timelines and actions taken.

This initial investigation should be completed urgently and wherever possible within 24 hours of the breach being discovered/reported. A further in-depth review of the causes of the breach and recommendations for future improvements can be undertaken once the matter has been resolved.

2.2 Assessing the risk

Before deciding on what steps are necessary further to immediate containment, assess the risks which may be associated with the breach. Most important is an assessment of potential

adverse consequence for individuals, how serious or substantial these are and how likely they are to happen.

When making the assessment the following need to be considered:

- What type of data is involved?
- How sensitive is the data involved?
- If data has been lost or stolen, are there any protections in place such as encryption?
- What has happened to the data? If data has been stolen, it could be uses for purposes which are harmful to the individuals to whom the data relate; if it has been damaged, this poses a different type and level of risk.
- Regardless of what has happened to the data, what could the data tell a third party about the individual? Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people.
- How many individuals' personal data are affected by the breach? It is not necessarily the case that the bigger risks will accrue from the loss of large amounts of data but is certainly an important determining factor in the overall risk assessment.
- Who are the individuals whose data has been breached? Whether they are staff, customers, clients or suppliers, for example, will to some extent determine the level of risk posed by the breach and, therefore, your actions in attempting to mitigate those risks.
- What harm can come to those individuals? Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
- Are there wider consequences to consider such as a risk to public health or loss of public confidence in an important service you provide?
- If individuals' bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help you prevent fraudulent use.

2.3 Notification of breaches

Notification should have a clear purpose, whether this is to enable individuals who may have been affected to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints. From 26 May 2011 certain organisations (service providers) have a requirement to notify the Information Commissioner, and in some cases individuals themselves, of personal data security breaches. For more information about the specific breach notification requirements for service providers see:
https://icosearch.ico.org.uk/s/search.html?query=breach+notice+requirements&collection=ico-meta&profile=_default

The following should be considered in deciding whether, and whom, to notify:

- Are there any legal or contractual requirements?
- Can notification help to meet security obligations with regards to the data protection principles?
- Can notification help the individual?
- Can they act on the information to mitigate risk?

- Is there a large number of people affected, or are there very serious consequences? If yes to either, the ICO should be informed immediately.
- How can notification be made appropriate for particular groups or individuals, for example, if data concerns children or vulnerable adults.
- Is there a danger of 'over notifying'? Not every incident will warrant notification.

In order to assess who to notify, what information needs to be communicated and how, the following will be observed:

- Notify the appropriate regulatory body.
- Chose the most appropriate way to notify those affected, considering security of the medium as well as the urgency of the situation.
- Notifications should include, but not be limited to:
    - How the breach occurred?
    - When the breach occurred?
    - What data was involved?
    - What has been done to respond to the risk posed by the breach?
    - Advice, if necessary and possible, on the steps that can be taken for protection of mis-use and also what PFA Research can do to help.
    - Provision of lines of communication for further contact to obtain further information, e.g. a helpline number, web page or dedicated email address.

When notifying the ICO information should also be included, but not limited to:

- Security measures in place, such as encryption.
- Details of security procedures in place at the time of breach.
- Media awareness.

Other third parties to notify if necessary are

- The police
- Insurers
- Professional bodies
- Bank or credit card companies
- Trade unions

2.4 Review and Evaluation

Once the initial aftermath of the breach is over, the Data Protection Officer together with the Managing Director should fully review both the causes of the breach and the effectiveness of the response to it. If systemic or ongoing problems are identified, then an action plan must be drawn up to put those right.

This policy and the procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance. It is the responsibility of the Data Protection Officer and the Managing Director to ensure that this policy is kept up–to-date.

3 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.

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.

4 References

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

- PFA Research UK GDPR Policy
- Information Security Policy
- Email and Internet Policy
- Business Continuity Management Plan
- Emergency Response Plan
- Procedures for processing and handling samples containing personal data

5 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.

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

6 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

7 Version History

Reviewed	Next Review	Reviewed by
July 2014	July 2015	Beate Galke – Project Manager
March 2015	March 2016	Beate Galke – Project Manager. Note: Policy has been aligned with the guidelines published by ICO.
April 2017	April 2018	Beate Galke – Project Manager. Note: Policy needs to be updated as necessary with the recent changes to the data protection act (DGPR). BG to investigate and make necessary changes as required.
May 2018	May 2019	Beate Galke – Operations Manager
May 2019	May 2020	Beate Galke – Operations Manager
August 2020	December 2020	Beate Galke – Operations Manager – to be reviewed when further information on EU Exit regulations are available.
December 2020	December 2021	Beate Galke – Operations Manager – no further information available.
October 2021	October 2022	Beate Galke – Operations Manager
May 2022	May 2023	Beate Galke – Operations Manager Policy review following change to MS365
May 2023	May 2024	Beate Galke – Operations Manager and DPO
May 2024	May 2025	Beate Galke – Operations Manager and DPO
June 2025	June 2026	Beate Galke – Operations Manager and DPO