PAM Group Ltd

HP013 - Data Protection Policy

28/05/2025

Contents

Document Change Control

Version	Date	Author	Approver	Change Detail
1 to 5	April 24	Tara Wise	Jim Murphy	Original DP Policies
5.1	13/02/25	Pippa Boulton	DPO	Creation/authoring of Policy
5.2	17/02/25	Pippa Boulton	DPO	Additional sections added
5.3	13/03/25	Pippa Boulton	DPO	Further review and amends
5.4	17/03/25	Pippa Boulton	DPO	Review and added in extra sections
5.5	23/05/2025	Pippa Boulton	DPO	Final sense check
6.0	28/05/2025	Pippa Boulton	DPO	Published

Policy Owner: Pippa Boulton, Data Protection Officer (DPO)

Review Frequency: Annually, or a full policy review could be triggered after a serious data breach or after legislation changes, or important changes in case law or guidance.

Next Scheduled Review: 28/05/2026

Approved by: Pippa Boulton, Data Protection Officer (DPO)

Distribution: Internal and External

This Policy will be continuously assessed against new technologies, business practices, regulatory changes and the evolving needs of the business and the services we provide.

For any queries regarding this policy, please contact the policy owner.

1. Purpose

The purpose of this policy is to establish guidelines and to provide a framework for ensuring that PAM Group (hereafter referred to us "PAM") meets its obligations under the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (DPA18).

PAM complies with data protection legislation guided by data protection principles as described in UK GDPR[1]. In summary, these principles require us to:

1. Process all data fairly, lawfully and in a transparent manner.
2. Obtain data for specified purposes and then only used for those purpose and not use or disclose that data in anyway incompatible with those purposes.
3. Adequate, relevant, and not excessive
4. Accurate, and where necessary, up to date.
5. Not kept for longer than is necessary.
6. Data is kept safe and secure.

In addition, PAM follows the accountability principle that requires us to evidence our compliance with the above 6 principles and ensure that we do not put individuals at risk because we are processing their personal data. Failure to follow these principles, can result in:

- Breach of legislation
- Reputational damage
- Financial implications to the Company, due to fines

To meet our obligations, we put in place appropriate and effective measures to make sure we comply with data protection legislation.

2. Scope

This policy applies to all the processing of personal data carried out by PAM including processing carried out by joint controllers, contractors, and processors.

This policy applies to clients, their employees, our colleagues, job applicants, suppliers, third party contractors, volunteers, and any regulatory authority.

[1] GDPR is a European legislation that the UK adopted into UK law (UK GDPR) following the United Kingdom's European Union (Withdrawal) Act 2018.

3. Policy Statement

PAM maintains up to date registration with the Information Commissioner's Office as required by law.

All contracts between PAM and external data processors are reviewed by the Data Protection Officer for compliance with Data Protection Act requirements.

All individuals covered by this policy must abide by the procedures herewith and acknowledge their requirements in relation to data incidents. Individuals must:

- Report all data protection incidents to the Data Protection Team (data.protection@pamgroup.co.uk) as soon as they are made aware of the incident, however long ago it appears to have occurred, and where possible within 24 hours.

4. Information that is covered by Data Protection Legislation

4.1 Personal Data

The UK GDPR definition of "personal data" includes any information relating to an identified or identifiable natural living person. The full definition I defined as:

> "'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

Pseudonymised personal data is covered by the legislation, however anonymised data is not regulated by the UK GDPR or DPA 18, providing the anonymisation has not been done in a reversible way.

4.2 Special Category Data (sensitive)

Some personal data is more sensitive and is afforded more protection, this is information related to:

- Race or ethnic origin.
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data

- Biometric ID data
- Health data
- Sexual life and/or sexual orientation

4.3 Criminal data (convictions and offences)

The UK GDPR gives extra protection to "personal data relating to criminal convictions and offences or related security measures." This covers a wide range of information about offenders or suspected offenders in the context of:

- criminal activity
- allegations
- investigations
- proceedings

It includes not just data which is obviously about a specific criminal conviction or trial, but may also include personal data about:

- unproven allegations
- information relating to the absence of convictions.

It also covers a wide range of related security measures, including:

- personal data about penalties
- conditions or restrictions placed on an individual as part of the criminal justice process.
- civil measures which may lead to a criminal penalty if not adhered to

It does not cover information about other individuals, including victims and witnesses of crime. However, information about victims and witnesses is likely to be sensitive, and as a data controller particular care is required when processing it.

5. Legal bases for processing data

We hold and process information in relation to the occupational health and wellbeing services we offer to our clients, their employees and to our own employees. We therefore rely on the following legal bases for processing data as set out in the Data Protection Act – UK (2018) and the Regulation (EU) 2016/679 (General Data Protection Regulation) (UK GDPR)[2].

[2] GDPR is a European legislation that the UK adopted into UK law (UK GDPR) following the United Kingdom's European Union (Withdrawal) Act 2018.

UK GDPR Article (6)(1)(b) - Processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering into a contract; And or

UK GDPR Article 9(2)(h) - Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems.

Data Protection Act – UK (2018) Schedule 1 Part 1 s(2)

> *"Health or social care purposes.*
>
> *2 (1) This condition is met if the processing is necessary for health or social care purposes.*
>
> *2 (2) In this paragraph "health or social care purposes" means the purposes of.*
>
> *(a) Preventative or occupational medicine*
>
> *(b) The assessment of the working capacity of an employee,*

6. Responsibilities

6.1 Board of Directors

The Board of Directors of PAM Group recognises its overall legal responsibility for Data Protection compliance. Day to day responsibility for Data Protection is delegated to the Data Protection Officer.

6.2 Data Protection Officer

The main responsibilities of the Data Protection Officer are:

- Briefing the Board on their and PAM's Data Protection responsibilities.
- Reviewing Data Protection and related policies.
- Advising our colleagues on Data Protection issues.
- Ensuring that Data Protection induction and regular training takes place.
- Reviewing contracts with Data Processors (external contractors and suppliers of outsourced services).
- Notification (i.e. registration with the Information Commissioner).
- Management of subject access requests from individuals for access to their personal data.

6.3 Operation Directors and Senior Management

PAM operational Directors and Senior Management Team have responsibility for data protection within their own area of operation.

6.4 Colleagues

All our Colleagues are responsible for ensuring information and data is maintained securely in accordance with this policy and procedures that apply to their area of work.

All our Colleagues have the following responsibilities:

- Assisting the Data Protection Officer in identifying aspects of their area of work which have Data Protection implications so that guidance can be provided, as necessary.
- Ensuring that their activities take full account of Data Protection requirements.
- Engaging fully in Data Protection and confidentiality training.

7. Confidentiality and Security

PAM recognises that a clear policy on confidentiality of personal data – in particular that of users – underpins security. It maintains a policy that sets out how our colleagues are authorised to access, which data, and for which purposes.

All colleagues are required to abide by any security measures designed to protect personal data from loss, misuse or inappropriate disclosure or processing data for any other reason other than the delivery of services that the Company has accepted.

7.1 Privacy Policy (Notice)

We publish a privacy policy on our websites and provide updates when required. We make changes to our Privacy Policy when there are amendments to law, changes in processes, changes in who we share data with. Our Privacy Notice contains contact details for our Data Protection Officer (DPO) and explains the purposes for which personal data is collected and used and our legal basis for processing.

7.2 Training

PAM will ensure that **ALL** staff with access to personal data have received appropriate data protection training and are aware of the confidential nature and duties placed on those processing identifiable personal and special category data as well as pseudonymised data. This includes ensuring we have appropriate training, monitoring, policies, and procedures in place for all staff. PAM will remain responsible for the processing of data by its sub processors or Associates on the same basis as if PAM was the data processor. PAM will control the processing of any sub processors or Associates.

We require all PAM employees and Associates to undertake mandatory annual training. In addition, all staff are required to attend a more detailed data protection training module as part of their induction or retake the training if there has been a data incident or potential/actual data breach caused by human error.

7.3 Data Incidents and Breaches

We consider all personal data incidents and have a reporting mechanism that is communicated to all staff. The Data Protection Team will assess all data incidents to determine if the reported incident is a potential or actual data breach. The Data Protection Team will then assess whether we need to report breaches to the ICO as the Regulator of the Data Protection Act UK (2018). We will also take appropriate action to make data subjects aware if needed.

7.4 Data Protection by Design and default

We follow a procedure of due diligence to assess the processing of personal data perceived as high risk, which will then require a Data Protection Impact Assessment (DPIA) to be carried out. We also have processes to assist staff in ensuring compliance and privacy by design is an integral part of any product, project, or service that we offer.

7.5 Records of Processing Activities (ROPAs)

We record our processing activities and publish our safeguards policy on law enforcement processing and processing of special category data.

7.6 Policies and Procedures

We produce policies and guidance on information management and compliance that we communicate to staff. Any change or update to a policy or procedure will be communicated to all staff and published on the intranet. For those documents that are required for external publication these will be published at the earliest opportunity.

7.7 Communications

We have a clear communication plan which seeks to embed a culture of privacy and risk orientation.

7.8 Contracts

Our Data Protection Team oversee that our contracts are compliant with UK GDPR and work closely with our teams to ensure that all contracts are appropriate. Our standard contracts for PAM will be reviewed on an annual basis, but sooner if there is any applicable change in legislation that requires our standard contracts to be amended and/or updated.

8. Data Storage and Retention

Steps are taken throughout PAM, both organisational and technical, to ensure that personal and special category data that we process is held securely and protected against loss or misuse. All Data is stored on secure servers in either the United Kingdom or the Republic of Ireland dependent upon a client's home operation and operated by Amazon Web Services (AWS). Specific data retention types and retention periods are listed in the Group Records Management Policy, **which is currently under development**.

9. Monitoring & Enforcement

Adherence to this policy is monitored by the Data Protection Team. Violations to this policy may result in corrective action, revocation of access/permission, disciplinary action against the user, and regulatory offences that may result in fines or action being taken against the organisation.

Definitions & Acronyms

Term	Definition
Data Controller	Means a person, or organisation, who controls the purpose of and means by which personal and sensitive data is processed. A Data Controller is responsible for complying with data protection regulations and remains accountable for the processing even if a third party carries it out on their behalf. The legal definition of a data controller is given in Art. 4(7) UK GDPR.
Data Processor	Means a natural, or legal person/organisation, public authority, agency, or other body which processes personal data on behalf of the Data Controller.
DPA	Data Processing Agreement
DPA 18	Data Protection Act – UK (2018)
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
ICO	Information Commissioner's Office - UK
Independent Controllers	Means a party which is a data controller of the same personal data as the other party and there is no element of joint control with regards to the personal data.
Joint Data Controllers	Means where two or more organisations will work together by jointly determining "why" and "how" personal data should be processed
UK GDPR	UK General Data Protection Regulation

Related Policies & References

Reference	Location/Name
Information Security Incident Mgmt. Policy	Internal/SharePoint and external
PAM Group Privacy Policy	Externally shared on our various websites
Data Breach Management Policy	Internal/SharePoint
Group Records Management Policy	In development