

---

Corporate Governance & Compliance  
Policy, Procedures and Standards

# DATA PROTECTION POLICY

*Document Ref: ISP-001*

*Last revision: Thursday, May 17, 2018*

*Next review date: Wednesday, May 01, 2019*



Panther Warehousing Limited,  
Lodge Farm Industrial Estate,  
Northampton,  
Northamptonshire.  
NN5 7US

## Document Control

Version:	3.0 (PUBLISH)
Date:	4 <sup>th</sup> May 2018
Owned by:	IT Department
Author:	Sarah Dommett
Reviewer:	HR – Hicks Watson
Document ID	Panther_Data_Protection_Policy_001

## Review and Update Policy

The document owner will review and update this Data Protection Policy on at least an annual basis.

# Contents

1.	Policy Statement .....	4
1.1.	Policy Scope .....	4
1.2.	Background .....	4
2.	Definition of Personal Data .....	5
2.1.	Responsibilities with regard to processing Personal Data .....	5
2.2.	Penalties for Breach of Data Protection Laws .....	5
2.3.	Access to Personal Data .....	6
2.4.	Employee Personal Data .....	6
2.5.	Sensitive Personal Employee Information .....	6
2.6.	Transmitting Personal Data securely .....	7
2.7.	Securing Personal Data .....	7
3.	Monitoring .....	8
4.	Enforcement .....	8

# 1. Policy Statement

This policy is designed to clarify and provide guidance on the Data Protection Laws. This policy will be reviewed in line with any changes to the laws and redistributed where required. A summary of areas covered by this policy are detailed below. Should you have any questions in relation to this document, please speak to your Line Manager: -

- General principles of the Policy;
- Definition of Personal Data;
- Responsibilities with regard to processing and access to Personal Data;
- Penalties for breach of Data Protection Laws;
- Access to Personal Data;
- Employee personal and sensitive information;
- Transmitting and monitoring.

Panther Warehousing Limited (Panther) has separate privacy notices in place in respect of employees, customers/clients, and other categories of data subject., the privacy notices will always be communicated clearly, and will inform the data subject of how their data will be processed and the reasons for processing that data. A copy of Panther's privacy notice can be obtained on Cascade, via the website or upon request from the DPO.

## 1.1. Policy Scope

It is Panther's approach that personal information is: -

- Used fairly and lawfully;
- Used for limited specifically stated purposes;
- Used in a way that is adequate, relevant and not excessive;
- Accurate;
- Kept for no longer than is absolutely necessary;
- Kept safe and secure;
- Not transferred outside the UK without adequate protection.

This is in line with all Data Protection Laws and the principles contained within these laws. Panther is accountable for these principles and must be able to demonstrate and maintain compliance with these principles and laws at all times.

## 1.2. Background

The rules in this policy apply to all employees, contractors, sub-contractors and temporary workers that work for Panther.

During the course of employment with the company, employees may come into contact with and use confidential personal information about staff and client customers, such as names and addresses or even information about their circumstances, families, health and other private matters.

Staff processing personal data on behalf of Panther have a responsibility to treat such data in line with Data Protection Laws and as directed by Panther (the Data Controller). Panther will comply with its obligations under the Data Protection Laws.

## 2. Definition of Personal Data

Personal Data is information about a living person who can be identified by that information, or by other information which is in the possession of Panther. Information includes any expression of opinion about the individual, and any indication of the intentions of the Company, or another person about the individual. Within Panther this can include information about employees or workers with Panther, or customer information and records or any other Personal Data.

The Data Protection laws apply whether the information is in removeable media, hardcopy or electronic format.

### 2.1. Responsibilities with regard to processing Personal Data

"Processing" personal data includes obtaining, recording, organising, adapting, altering, retrieving, consulting, using, holding, disclosing, publishing, aligning, combining, blocking, erasing or destroying personal data.

Processing should be fair and lawful. To be fair and lawful, it should only be used in a way the individual reasonably expects and that the individual has been made aware of which company (including any third parties to whom it may be disclosed) is processing the data. This includes providing information to third parties providing services to Panther.

The Data Protection laws provide strict rules in the relation to processing such Personal Data about data subjects. If employees are in any doubt about what they may or may not do, they should seek advice from their Manager. If employees are in doubt and cannot get in touch with their Line Manager or the HR Administrator, the information concerned must not be disclosed.

Employees must not provide personal data to any third party (that isn't a standard Subject Access Request) unless this has been specifically agreed by the Data Protection Officer.

If you become aware or have reason to suspect that personal data has been released or compromised in any way, or there has been a potential breach of the Data Protection Laws, you should contact the IT Department immediately. You will receive advice on what to do next when you ring.

Staff processing Personal Data on behalf of Panther have a responsibility to treat such data in line with the Data Protection Laws and as directed by Panther (the Data Controller). Personal data staff may come into contact with during their working responsibilities must be kept secure and confidential at all times.

### 2.2. Penalties for Breach of Data Protection Laws

Panther itself and individual employees may be personally liable to fines and criminal prosecution in the event of a breach of data protection regulations. Fines for breaches of data protection are potentially unlimited in the Crown Court and have been increasing both for Companies and individuals in recent years, as the Government and Courts approach the issue. This approach has only been reinforced with the introduction of the **General Data Protection Regulation (GDPR) (EU) 2016/679**.

There are two levels of potential fines that can be levied;

- Up to €10 million, or 2% annual global turnover – whichever is greater;
- Up to €20 million, or 4% annual global turnover – whichever is greater.

## 2.3. Access to Personal Data

Employees and others about whom Panther holds Personal Data (Data Subjects) may request to inspect personal information (a Subject Access Request) which Panther holds in relation to them and request that any inaccuracies are corrected.

Additionally, Subject Access Requests can be made by other organisations, in particular where illegality or criminality of the Data Subject is suspected.

Request from clients or customers of the clients should be sent to [dpo@panthergroup.co.uk](mailto:dpo@panthergroup.co.uk) where the Data Protection Officer will handle them.

Any member of staff dealing with enquiries from third parties should be careful about disclosing any personal information held by the Company. In particular they should: -

- Request that the third party put their request in writing so the third party's identity and entitlement to the information may be verified;
- Check the identity of the person making the enquiry and whether they are legally entitled to receive the information they have requested;
- Refer to their line manager or the HR Administrator for assistance in complex situations.

Employees who wish to make an access request should put their request in writing to [hrenquiries@panthergroup.co.uk](mailto:hrenquiries@panthergroup.co.uk)

- The IT department and HR department will manage these requests and Data will be checked for via tracker, archives and keyword search in emails;
- Data will be sent via one of the secure transmission procedures;
- All third-party information, where applicable, will be redacted;
- Request and outcome of request to be logged for monitoring purposes.

## 2.4. Employee Personal Data

It is important that employees immediately notify any changes in personal information to their Manager. These include changes to Personal Data as part of employment which generally covers the following: -

- Change of name;
- Change of address and telephone number;
- Change to dependants (e.g. for parental and emergency leave requests);
- Change of name and contact details of next of kin and persons to be notified in case of emergency if different;
- Change in professional and educational qualifications (for validation and legislation);
- Changes to tax code and National Insurance number (for payroll purposes);
- Changes to bank account (for Salary payment);
- Changes to driving license (where relevant to the employee's role/claims);
- Evidence of entitlement to work in the UK;
- Change to nominated beneficiaries (where applicable).

## 2.5. Sensitive Personal Employee Information

Panther may also hold sensitive personal information on its employees, including any of the following kind, any changes to which (as appropriate) must be notified to the Line Manager immediately: -

- Racial or ethnic origins (focused on equal opportunity monitoring);
- Religious beliefs or similar (focused on equal opportunity monitoring and medical needs);
- Trade union membership (focused on union administration purposes);
- Physical or mental health (focused on SSP, SMP, equal opportunities monitoring and employment administration purposes);
- Commission (or alleged commission) of an offence (focused upon detection of misconduct and employment administration purposes).

Panther will ensure that sensitive information is securely held and properly administered in accordance with the laws.

It is important that changes in personal circumstances (including the above personal and sensitive data) are notified to the Line Manager immediately.

## 2.6. Transmitting Personal Data securely

All employees should be aware of the risks when transmitting Personal Data. Particular care must be taken over customer records. The following guidance is for employees responsible for Personal Data: -

- ! Pay particular attention to the risks of transmitting confidential employee information by email;
- ! Email attachments including personal data for customers must be password protected following the password management policy set out in Acceptable Use policy;
- ! Transmit information between locations only if a secure network or comparable arrangements are in place or if, in the case of email, encryption is used;
- ! All copies of email and fax messages received by managers should be held securely;
- ! Fax transmission is not secure and must be avoided wherever possible;
- ! Envelopes must be securely sealed, clearly addressed to a known contact and marked “confidential” and “addressee only”. A return postal address should also be marked on the envelope;
- ! When anonymised or pseudonymised information is shared, care must be taken to ensure that the method used is effective and individuals cannot be identified from the limited data set e.g. age and postcode together could be sufficient enough to reveal an individual’s identity.

In accordance with Panther’s legal obligations under TUPE legislation, if Panther sells all or part of its business, it may provide Personal Data about employees to any prospective purchaser in the course of negotiations. As far as possible, such data will be provided in an anonymous form and if this is not possible, the prospective purchaser will be required to keep the information confidential. We will transfer any Personal Data on any transfer or sale falling within the terms of the Transfer of Undertakings (Protection of Employment) Regulations.

## 2.7 Securing Personal Data

Employees should only access personal data within Panther if it is required for the performance of your workplace duties, and only if you have the authorisation to do so by a line manager. On this point, it is important to note that personal data should only be used for the specified lawful purpose for which it was obtained.

- Personal data must never be shared informally.
- You have a responsibility to keep personal data secure and not share it with unauthorised people.
- You should not make unnecessary copies of personal data and you must dispose of any copies securely.
- You must lock your computer screens when not at your desk in accordance with the Clear Desk, Clear Screen policy.

- Consider anonymising data or using separate keys/codes so that the 'data subject' cannot be identified before sending the data.
- Do not save personal data to your own personal computers or other devices or your local laptop/PC drive.
- You should lock drawers and filing cabinets. Do not leave paper with personal data lying about in accordance with the Clear Desk, Clear Screen policy.
- You should not take personal data away from Panther's premises without authorisation from your line manager or IT Department.
- Personal data should be disposed of securely in the confidential waste bins when you have finished with it.
- You should ask for help from your line manager if you are unsure about data protection or if you notice any areas of data protection or security that Panther can improve upon.

### 3. Monitoring

Panther may monitor emails and telephone calls made via business systems but strictly in accordance with what is permitted under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. Employees are made aware of any such monitoring within the Employee Privacy notice and/or the Employee Handbook.

Any data protection queries should be addressed to the HR Administrator.

### 4. Enforcement

Any deliberate or negligent breach of this policy by you may result in disciplinary action in accordance with Panther's disciplinary procedure, and it is important that you are aware that any such deliberate or negligent actions may amount to Gross Misconduct and could result in your dismissal. Other forms of remedial action can be taken where appropriate, such as is the case with contractors and workers.

It is a criminal offence to conceal or destroy personal data which is part of a subject access request. This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in dismissal.