



DATA PROTECTION POLICY

1. Context & Overview Introduction

Pangeotek needs to gather and use certain information about individuals. This can include customers, suppliers, business contacts, employees and other people the company has a relationship with or may need to contact.

Pangeotek is committed to a policy of protecting the rights and privacy of individuals in accordance with the General Data Protection Regulations (GDPR) May 2018. The new regulatory environment demands higher transparency and accountability in how we manage and use personal data. It also accords stronger rights for individuals to understand and control that use.

To comply with various legal obligations, including the obligations imposed on it by the General Data Protection Regulation (GDPR), Pangeotek must ensure that all this information about individuals is collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. This policy describes how the personal data must be collected, handled and stored to meet the company's data protection standards and to comply with the law.

Why This Policy Exists

This data protection policy ensures that Pangeotek:

- Complies with the data protection law and follows good practice
- Protects the rights of staff, customers and suppliers
- Is open about how it stores and processes individual's data
- Protects itself from the risks of a data breach

Data Protection Law

The General Data Protection Regulation (GDPR) came into force on the 25th May 2018. The DPR regulates the processing of personal data and protects the rights and privacy of all living individuals (including children), for example by giving all individuals who are the subject of personal data a general right of access to the personal data which relates to them. Individuals can exercise the right to gain access to their information by means of a 'subject access request'. Personal data is information relating to an individual and may be in hard or soft copy (paper/manual files; electronic records; photographs; CCTV images) and may include facts or opinions about a person.

2. Risks and Responsibilities

Data Protection Risks

This policy helps to protect Pangeotek from some very real data security risks including:

- Breaches of confidentiality. For instance, information being given out inappropriately

- Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them, including whether the data is used for marketing purposes
- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities under the GDPR

Everyone who works for or with Pangeotek has some responsibility for ensuring that data is collected, stored and handled appropriately. Pangeotek will be the 'data controller' under the terms of the legislation – this means that it is ultimately responsible for controlling the use and processing the personal data.

The company has appointed a Data Protection Officer (DPO), currently the Office Manager, who is available to address any concerns regarding the data held by the company and how it is processed, held and used. The DPO is also responsible for:

- Reviewing all data protection procedures and related policies in line with an agreed schedule
- Handling data protection questions from individuals covered by the policy
- Dealing with requests from individuals to see data.
- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly
- Evaluating any third-party services the company is considering using to store or process data. For instance, Cloud computing services.
- Working with other staff to ensure marketing initiatives abide by data protection principles.
- Approving any data protection statements attached to communications such as emails.

The Management Team is responsible for all day-to-day data protection matters and will be responsible for ensuring that all members of staff and relevant individuals abide by this policy and for developing and encouraging good information handling within the company.

3. General Staff Guidelines

- The only people able to access data covered by this policy should be those who need it for their work
- Employees should keep all data secure by taking sensible precautions and following the guidelines below
- In particular, strong passwords must be used, and they should never be shared
- Personal data should not be disclosed to unauthorised people, either within the company or externally
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from the DPO if they are unsure about any aspect of data protection.

4. Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the DPO.

When data is stored on paper it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason.

- When not required the paper or files should be kept in a locked drawer or filing cabinet
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer or photocopier.
- Data printouts should be when no longer required.

When data is stored electronically it must be protected from unauthorised access, accidental deletion and malicious hacking attempts.

- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removeable media (like a DVD or portable hard drive) these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers and should only be uploaded to approved cloud computing services
- Data should be backed up frequently. Those backups should be tested regularly to ensure the integrity of the data.
- All computers containing data should be protected by an approved security software and a firewall.

5. Data Use

Personal data is of no value to Pangeotek unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss or theft.

When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.

Personal data should not be shared informally. In particular, it should never be sent by email as this form of communication is not secure.

6. Data Accuracy

The law requires Pangeotek to take reasonable steps to ensure data is kept accurate and up to date. The more important it is that the personal data is accurate, the greater the effort Pangeotek should put into ensuring its accuracy. It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible

Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.

Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.

Pangeotek will make it easy for data subjects to update the information that Pangeotek holds about them. For instance, this can be done via the company website.

Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

7. **Subject Access Requests**

All individuals who are the subject of personal data held by Pangeotek are entitled to:

- Ask what information the company holds on them and why
- Ask how to gain access to that information
- Be informed how to keep it up to date
- Be informed how the company is meeting its data protection obligations

If an individual contacts the company requesting this information, this is called a subject access request. Subject access requests from individuals should be made by email, addressed to karen.white@pangeotek.com. The data controller will always verify the identity of anyone making a subject access request before handing over any information. There is no charge for a subject access request and Pangeotek will arrange for an individual to see all the personal data held on them within 1 month of receipt of a written request.

8. **Disclosing Data**


For other reasons and in certain circumstances it is permissible for personal data to be disclosed to a law enforcement agency without the consent of the data subject. Under these circumstances, Pangeotek will disclose the requested data. However, the data controller will ensure that the request is legitimate, seeking assistance from the company's legal advisers where necessary.

9. **Providing Information**

Pangeotek aims to ensure that individuals are aware that their data is being processed and that they understand:

- How the data is being used
- How to exercise their rights

To these ends the company has a Privacy Statement setting out how data relating to individuals is used by the company. This is available on request and is also available on the company website.



Lee White
Director/Senior Consultant
Pangeotek Ltd