Scientific.
GROUP

Data Protection Policy

March 2023

Contents

1. General guidelines 3
2. Data protection law 3
3. Policy scope 5
4. Data protection risks 5
5. Responsibilities 5
6. General staff guidelines 6
7. Data storage 7
8. Data use 8
9. Data accuracy 8
10. Subject access requests 9
11. Disclosing data for other reasons 10

Sceintific Group refers to all associated companies and subsidiaries, and will be referred to as the Company herein.

The UK Data Protection Act 1998 applies to every business that collects, stores and uses personal data relating to customers, staff or other individuals.

Failing to follow the rules could mean criminal sanctions or a fine of up to £500,000.

A clear data protection policy makes sure everyone in the Company understands why data protection is important. It also describes procedures for collecting, working with and storing data.

This policy is subject to the Company's discretion and is in line with the Company's IT and Communications Usage Policy.

This policy does not form part of any employee's employment contract. It will be reviewed and amended as necessary in line with Government advice. However, all data users are obliged to comply with this policy when processing personal data on our behalf and any breach of this policy may result in disciplinary action.

1. General Guidelines

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

This policy describes how this personal data must be collected, handled and stored to meet the Company's data protection standards and to comply with the law.

This data protection policy ensures the company:

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

2. Data Protection Law

The Data Protection Act 1998 describes how organisations must collect, handle and store personal data.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not be disclosed unlawfully.

The Data Protection Act is underpinned by 8 important principles.

- Be processed fairly and lawfully
- Be obtained only for specific, lawful purposes
- Be processed for limited purposes and in an appropriate way
- Be accurate and kept up to date
- Not be held for any longer than necessary
- Processed in accordance with the rights of data subjects
- Be protected in appropriate ways
- Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection.

The Act provides conditions for the processing of any personal data. It also makes a distinction between personal data and "sensitive" personal data. Personal data is defined as, data relating to a living individual who can be identified from:

- That data
- That data and other information which is in the possession of, or is likely to come into our possession.

Sensitive personal data is defined as personal data consisting of information as to:

- Racial or ethnic origin;
- Political opinion;
- Religious or other beliefs;
- Trade union membership;
- Physical or mental health or condition;
- Sexual life;
- Criminal proceedings or convictions.

3. Policy Scope

This policy applies to:

- The AS&K Group - all associated companies and subsidiaries
- All staff and volunteers
- All contractors, suppliers and other people working on behalf of the Company

It applies to all personal data that the Company holds relating to identifiable individuals as covered by the Data Protection Act. Personal data can include factual information such as:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers

It can also include opinions about a person, their actions or behaviour.

4. Data Protection Risks

This policy helps to protect the Company from data risks, including:

- Breaches of confidentiality – such as 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
- Reputational damage – for instance the company could suffer if hackers successfully gained access to sensitive data.

5. Responsibilities

Everyone who works for or with the Company has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

The Data Protection Compliance Manager is responsible for ensuring compliance with the Data Protection Act and with this policy. That post is held by

Roberta Crafford, HR Director, roberta.crafford@asandk.com. Any questions about the operation of this policy or concerns that this policy has not been followed should be referred in the first instance to the Data Protection Compliance Manager.

The Data Protection Compliance Manager will work closely with all relevant personnel to ensure, as appropriate:

- All employees are trained with regards to data protection
- The Policy is updated
- All requests from individuals regarding data being held are addressed
- All systems, services and equipment used for storing data meet acceptable security standards
- Regular checks and scans are conducted to ensure security hardware and software is functioning properly.

6. General Staff Guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- The protection documentation which appears at Schedule 1 to this policy should be completed at the start of a project. Data should not be shared informally. When access to confidential information is required, employees can request it from their line manager.
- The Company will provide training to all employees to help them understand their responsibilities when handling data.
- 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, whether within the Company or externally.
- Data should be regularly reviewed and updated if it is found to be out of data. If no longer required, it should be deleted and disposed of.
- Employees should request help from their line manager if they are unsure about any aspect of data protection.

7. Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to IT or Data Protection Compliance Manager.

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
- Data printouts should be shredded and disposed of securely 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.
- If data is stored on removable media (DVDs, USB sticks etc), these should be kept locked away securely when not being use.
- Data should only be stored on designated drivers and servers, and should only be uploaded to an approved cloud computing service.
- Servers containing personal data should be sited in a secure location.
- Data should be backed up frequently, and tested regularly.
- Data should never be saved directly to laptops or other mobile devices, such as tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.
- Digital storage devices should be physically destroyed when no longer required.

8. Data Use

Personal data is of no value to the Company unless the business can make use of it.

We may share personal data we hold with any member of our group. We may also disclose personal data we hold to third parties (e.g.: in the event that we buy or sell any business or assets in which case data may be disclosed to the potential buyer or seller or if we or substantially all our assets are acquired by a third party).

It is when personal data is accessed and used that it can be at the greatest risk of loss, corruption 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 shred informally.
- Data must be encrypted before being transferred electronically.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.
- Data transferred outside of the EU must comply with the guidelines of the DPA and specific regulations relating to that location. Data transfer between the EU and USA must adhere to the EU-US Privacy Shield and in line with the ICO's guidance
    - https://ico.org.uk/media/for-organisations/documents/1529/assessing_adequacy_international_data_transfers.pdf

9. Data Accuracy

The law requires the Company 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 the Company 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 fewer places as necessary. Staff should not create any unnecessary additional data sets.

- Staff should take every opportunity to ensure data is updated, for example by confirming a customer's details when they call.
- The Company will make it easy for data subjects to update the information the company holds about them.
- Data should be updated as inaccuracies are discerned, for example, if a customer can no longer be reached on their stored telephone number, then it should be removed from the database.
- Those working with marketing databases must ensure they are checked against industry suppression files every six months.
- We will not keep data for longer than is necessary for the purpose or purposes for which it was originally collected. We will take all reasonable steps to destroy or erase from our systems all data which is no longer required.

10. Subject Access Requests

All individuals who are the subject or personal data held by the Company are entitled to:

- Prevent the processing of their data for direct marketing purposes
- Prevent processing that is likely to cause damage or distress to themselves or to anyone else.
- Ask what information the Company holds about them and why.
- Ask how to gain access to it and find out who data will be shared with.
- Be informed how to keep it up to date and ask to have inaccurate data changed.
- Be informed how the Company is meeting its data protection obligations.

If an individual contacts the Company requesting details of information held about them, this is called a subject access request.

Subject access requests from individuals should be made by email and addressed to the HR Director. Individuals will be charged £10 per subject access request and the information will be aimed to be presented within a reasonable timeframe, namely 14 days.

11. Disclosing Data For Other Reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed without the consent of the data subject. This may occur when processing is necessary for the performance of a contract with the data subject (e.g. pay roll) or in more unusual circumstances where disclosure to third parties is necessary in order to comply with a legal obligation or to protect our rights, property or safety of our employees, customers or others.

Under these circumstances, the Company reserves the right to disclose requested data, however, the data controller will ensure the request is legitimate, seeking assistance from the Data Protection Compliance Manager and from the Company's legal advisers where necessary.