GDPR - DATA PROTECTION POLICY
ANDROS UK

1. KEY DETAILS

- Policy prepared by : ANDROS UK Limited
- Approved by board / management on : 31st May 2023

2. INTRODUCTION

ANDROS UK needs to gather, and use, certain information about individuals.

These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

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

3. WHY THIS POLICY EXISTS

This data protection policy ensures that ANDROS UK LTD:

- 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

4. DATA PROTECTION LAW

The Company is fully committed to compliance with the requirements of the General Data Protection Regulation (GDPR), the Data Protection Act 2018 and all other data protection legislation currently in force. The legislation applies to anyone processing personal data which includes Andros UK Ltd.

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 disclosed unlawfully.

The Data Protection Legislation is underpinned by seven important principles. These say that personal data must:

1. Be processed lawfully, fairly and transparency
2. Be obtained only for specific, lawful purpose
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Be protected in appropriate ways
7. Be processed in accordance with the rights of data subjects
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

These principles must be observed at all times when processing or using personal information. Therefore, through appropriate management and strict application of criteria and controls, the Company will:

- observe fully the conditions regarding having a lawful basis to process personal information;
- meet its legal obligations to specify the purposes for which information is used;
- collect and process appropriate information only to the extent that it is necessary to fulfil operational needs or to comply with any legal requirements;
- ensure the information held is accurate and up to date;
- ensure that the information is held for no longer than is necessary;
- ensure that the rights of people about whom information is held can be fully exercised under the GDPR (i.e. the right to be informed that processing is being undertaken, to access personal information on request; to prevent processing in certain circumstances, and to correct, rectify, block or erase information that is regarded as wrong information);
- take appropriate technical and organisational security measures to safeguard personal information;
- ensure that personal information is not transferred outside the EU, to other countries or international organisations without an adequate level of protection.

5. POLICY SCOPE

This policy applies to all employees, agency personnel, subcontractors, suppliers and other individuals working on behalf of Andros UK Ltd regardless of location.

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection legislation. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Any other information relating to individuals considered to be personally identifiable information such as NHS number, date of birth.

6. DATA PROTECTION RISKS

This policy helps to protect Andros UK Ltd 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.
- **Reputational damage**. For instance, the company could suffer if hackers successfully gained access to sensitive data.

7. RESPONSIBILITIES

Everyone who works for, or with, Andros UK Ltd 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.

However, the people which have key areas of responsibility need to ensure that Andros UK meets its legal obligations:

- The **Board of Directors** needs to ensure that Andros UK meets its legal obligations and is responsible for:
  - Keeping updated about data protection responsibilities, risks and issues.
  - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
  - Arranging data protection training and advice for the people covered by this policy.
  - Handling data protection questions from staff and anyone else covered by this policy.
  - Addressing any data protection queries from journalists or media outlets.
  - Dealing with requests from individuals to see the data Andros UK Ltd holds about them (also called '*subject access requests*').
  - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

- The **Finance and Administration Director** is responsible for:
  - 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.
  - Keeping a well-managed archive of invoices with electronic records saved regularly.
  - Making sure that records are destroyed after a set retention period.
  - Being able to provide customers or suppliers with records of their personal data on request.
  - Making sure that all contractors and third parties' processors are aware of the new regulation and they updated their privacy policy in order to comply.
  - Keeping internal records of data processing using record management systems able to extract raw data and provide a full audit history of records kept.
  - On request, removing data held on a customer or supplier who withdraws consent for it to be kept. Ensuring every piece of relevant data is removed, and doing so in a way that doesn't impact other records.

- Informing customers or suppliers without undue delay once a breach has been identified.
- Evaluating any third-party services the company is considering using or is already using such as card providers, payment software, etc…

- The **Marketing Manager** is responsible for:
- Approving any data protection statements attached to communications such as emails and letters.
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.
- Evaluating any third-party services the company is considering using or is already using for marketing, PR or research purposes.

- The **People and Development Manager** is responsible for:
- Data regarding employees/candidates 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.
- Making sure the employees' rights related to personal data are respected (right of access to their data, right to have inaccurate data rectified, right to be forgotten...).
- Providing to employees more detailed information as to the how and why of the processing of HR-related personal data.
- Keeping records of all processing activities.
- Notifying the data protection regulator (ICO) about a personal data breach within 72 hours and the affected employees without undue delay if the breach is likely to result in a high risk to his/her rights and freedoms.

8. EMPLOYEES' PERSONAL INFORMATION

Throughout employment and for as long as it is necessary after the termination of employment, the Company will need to process data about employees. The kind of data that the Company will process includes:

- any references obtained during recruitment
- details of terms of employment
- payroll details
- tax and national insurance information
- details of job duties
- details of health and sickness absence records
- details of leave records
- information about performance
- details of any disciplinary and grievance investigations and proceedings
- training records
- contact names and addresses
- correspondence with the Company and other information that has been given to the Company

The data the Company holds will be for management and administrative use only but the Company may, from time to time, need to disclose some data it holds about employees to relevant third parties (e.g. where legally obliged to do so by HM Revenue & Customs, where requested to do so by employees for the purpose of giving a reference or in relation to maintenance support and/or the hosting of data in relation to the provision of insurance). The Company may, from time to time,

share personal data outside of the UK to the parent Company; when this is necessary only relevant data will be shared and in line with this policy and will be secure at all times.

In some cases the Company may hold sensitive personal data, which is defined by the legislation as special categories of personal data. For example, this could be information about health, racial or ethnic origin, criminal convictions, trade union membership, or religious beliefs. This information may be processed not only to meet the Company's legal responsibilities but, for example, for purposes of personnel management and administration, suitability for employment and to comply with equal opportunity legislation. Since this information is considered sensitive, the processing of such data will be done with high care and under security measures.

9. DATA SECURITY

Employees are responsible for ensuring that any personal data that they hold and/or process as part of their job role is stored securely.

Employees must ensure that personal information is not disclosed either orally or in writing, or via web pages, or by any other means, accidentally or otherwise, to any unauthorised third party.

Employees should note that unauthorised disclosure may result in action under the disciplinary procedure, which may include dismissal for gross misconduct. Personal information should be kept in a locked filing cabinet, drawer, or safe. Electronic data should be coded, encrypted, or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

When travelling with a device containing personal data, employees must ensure both the device and data is password protected. The device should be kept secure and where possible it should be locked away out of sight i.e. in the boot of a car. Employees should avoid travelling with hard copies of personal data where there is secure electronic storage available. When it is essential to travel with hard copies of personal data this should be kept securely in a bag and where possible locked away out of sight i.e. in the boot of a car.

10. GENERAL STAFF GUIDELINES

- The only people able to access data covered by this policy should be those who **need it for their work.**
- Data **should not be shared informally**. When access to confidential information is required, employees can request it from their line managers.
- **Andros UK Ltd will provide training** to 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.
- 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 their line manager if they are unsure about any aspect of data protection.

11. DATA STORAGE AND TRANSMISSION

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT 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 unauthorized people could see them**, like on a printer.

  - When documents containing personal information are moving between departments they should be enveloped and not left where unauthorised people can see them.

  - Where emails contain personal information senders must ensure recipients require the information for work purposes. Group emails are not to be used.

  - **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 and never shared between employees.

  - If data is **stored on removable media** (like a USB, CD or DVD), 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 an **approved cloud computing services**.

  - Servers containing personal data should be **sited in a secure location**, away from general office space.

  - Data should be **backed up frequently**. Those backups should be tested regularly, in line with the company's standard backup procedures.

- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.

- All servers and computers containing data should be protected by **approved security software and a firewall**.

12. DATA USE

Personal data is of no value to Andros UK 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, 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 shared informally**. In particular, it should never be sent by email, as this form of communication is not secure.

- Data must be **encrypted before being transferred electronically**. The IT manager can explain how to send data to authorised external contacts.

- Personal data **shouldn't be transferred outside of the European Economic Area**.

- Employees **should not save copies of personal data to their own computers**.

- Always access and update the central copy of any data.

13. DATA ACCURACY

The law requires Andros UK 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 Andros UK 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.

Andros UK will make it **easy for data subjects to update the information** the company holds about them. For instance, via the company website.

Data should be **updated when 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.

It is the Marketing Manager's responsibility to ensure **marketing databases are checked against industry suppression files** every six months.

14. SUBJECT ACCESS REQUESTS

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

- Ask **what information** the company holds about them and why.
- Ask **how to gain access** to it.
- 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 or by post.

Individuals may be charged a small administrative fee per subject access request. The company will aim to provide the relevant data within 30 days.

The company will always verify the identity of anyone making a subject access request before handing over any information.

A letter will normally be sent to the data subject within one month from the date of the request for access rights, right of rectification, right of cancellation, right to limitation of processing, right to the portability of data, right of opposition and right of opposition to be the subject of an automated individual decision or profiling.

The deadline for responding to the data subject may be extended by two months if the request is complex or if he/she makes numerous requests but the data subject must be informed within one month of the extension of the deadline and the reasons for the delay. If there is a justified reason not to respond to the request, the company must inform the data subject of the reasons for his inaction and of his right to lodge a complaint with the ICO.

A letter will be sent to the recipients of the data when the data subject has made a request for rectification or deletion of data or a request for a limitation of processing.

15. DISCLOSING DATA FOR OTHER REASONS

In certain circumstances, the Data Protection legislation allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, Andros UK will disclose requested data. However, the company will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

16. DATA BREACH

INFORMATION COMMISIONAR'S OFFICE (ICO) is the UK's independent authority set up to control and impose penalties for non-compliance with GDPR.

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransom ware, or accidentally lost or destroyed.

When a personal data breach has occurred, you need to establish the likelihood and severity of the **resulting risk to people's rights and freedoms**. If it's likely that there will be a risk then you must notify the ICO; if it's unlikely then you don't have to report it. However, if you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it.

Notification of personal data breaches needs to be done to the person concerned as soon as possible if the violation is a risk to the rights and freedoms of the person concerned.

Content of the notification: nature of the violation, contact information, consequences of the violation, measures taken to remedy the violation.

Exception: implementation of appropriate technical and organizational protection measures / taking of subsequent measures so that the risk is no longer likely to materialize / if it requires disproportionate effort (public communication instead).

Notification of personal data breaches needs to be done to ICO as soon as possible and no later than 72 hours after the knowledge of the violation, unless there is no risk to the rights and freedoms of the natural person.

Content of the notification: nature of the violation, approximate number of data subjects + data record, contact information, consequences of the violation, measures taken to remedy the violation.

17. QUESTIONS OR COMPLAINTS

Should you have any questions regarding this policy, please contact:

Stephanie LITTLE – People and Development Manager
Email: stephanie.little@androsuk.co.uk
DI: +44 (0) 1373 456083