AUTOGIRO
Global Mobility Services

DATA PRIVACY

AND

PROTECTION POLICY

AUTOGIRO
Global Mobility Services

Introduction

Autogiro needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees, and other people the organization 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.

Why this policy exists

This data protection policy ensures Autogiro:

- Complies with data protection best practices
- Protects the rights of staff, customers, and partners
- Is open about how it stores and processes individual`s data
- Protects itself from the risks of data breach

People, risks, and responsibilities Policy Scope

This policy applies to:

- The head office of Autogiro
- All staff of Autogiro
- All contractors, suppliers and other people working on behalf of Autogiro.

It applies to all data that the company holds relating to identifiable individuals. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Any other information relating to individuals

Data protection risks

This policy helps to protect Autogiro 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.

Responsibilites

Everyone who works at or on behalf of Autogiro, including contractors and suppliers, has some responsibility for ensuring data is collected, stored and handled appropriately.

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

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.
- Autogiro 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 unauthorized people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. Info longer required, it should be deleted and disposed of.
- Employees should request help if they are unsure about any aspect of data protection.

Data Storage

These rules describe how and where data should be safety stored.

When data is stored on paper, it should be kept in a secure place where unauthorized 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.
- Data printouts should be shredded and disposed of securely when no longer required.

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

- Data should be protected by strong password that are changed regularly and never shared between employees.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers.
- 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 the 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.
- Devices storing data should be physically destroyed when no longer in use.

Data usage and disclosure

Personal data is of no value to Autogiro 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, personal data should only be sent via email if the emails are encrypted.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.
- Data should only be provided to approve vendors.

Data 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.
- Autogiro will make it easy for data subjects to update the information Autogiro holds about them.
- 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.

Monitoring and Enforcement

- Employees will be provided a copy of this policy as part of their new hire paperwork.
- Periodic reminders of this policy will be provided to all employees.
- The Telecommunications Manager will review the policy as needed and make any revisions necessary.
- Upon revision the policy will be redistributed to all employees, suppliers, and clients.