

DATA PROTECTION POLICY

Introduction

ARQX Capital SA (hereafter: “The Company”) 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 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 The Company:

- Complies with data protection laws 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

Data Protection Regulations

The Swiss Federal Act on Data Protection (FADP) and the EU General Data Protection Regulation (GDPR) describe how organisations including The Company must collect, handle and store personal data.

Personal data is any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.

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

To comply with the applicable law(s), personal data must be collected and used fairly, stored safely and not disclosed unlawfully.

The FADP and GDPR are underpinned by important principles stating that personal data must:

- Be processed fairly and lawfully
- Be obtained only for specific, law purposes
- Be adequate, relevant and not excessive
- Be accurate and kept up to date
- Not be held for any longer than necessary
- Be protected in appropriate ways
- Not to be transferred outside Switzerland, unless that country or territory also ensures an adequate level of protection.

Policy scope

This policy applies to all staff, volunteers, contractors, suppliers and other people working on behalf of The Company.

Data protection risks

This policy helps to protect The Company 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.

Responsibilities

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

The Board of Directors is ultimately responsible for ensuring that The Company meets its legal obligations.

The Swiss Data contact person is responsible for:

- Keeping the board 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
- Dealing with requests from individuals to see the personal data The Company 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.

General staff guidelines

The only people able to access personal data covered by this policy should be those who need it for their work for The Company. Such data may only be collected and processed for the original purpose indicated for the provision of the financial services provided.

Employees and Third-party Service Providers undertake to store all personal data lawfully and securely by taking appropriate technical and organisational measures 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.
- Personal data should be regularly reviewed and updated if it is found to be out of date. If no longer required for the original purpose for which the data was processed, it should be deleted or rendered anonymous.

Data Storage

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

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

These guidelines also apply to personal 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 safe, 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.
- 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:

- Personal data are protected by strong passwords that are changed regularly.
- Use of antivirus software and malware protection that are updated frequently.
- Personal data are stored on the Cloud in Switzerland.
- No data can be exchanged between entities of the Group if they are abroad.
- The personal data are backed up frequently. These back-ups are also stored in a safe.

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 few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated.
- 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.

Subject Access Requests

All individuals who are the subject of personal data held by The Company 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 e-mail, addressed to the Swiss Data contact person (Pauline Hay) at pauline.hay@arqx-capital.com.

The Swiss Data contact person will aim to provide the relevant data within 14 days.

The Swiss Data contact person will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, the FADP and GDPR regulations allow personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, The Company will disclose requested data. However, the Swiss Data contact person will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.