Privacy Policy

Amstel Capital (Malta) Ltd ("ACM") and its affiliated Schemes Amstel Alternative Credit Fund SICAV plc ("AACF") and Amstel Global Umbrella Fund SICAV plc ("AGUF") implement and maintain systems and procedures to safeguard the security, integrity and confidentiality of information and data.

The three above mentioned entities are committed to safeguard the privacy of their Investors and employees treating personal information according to the General Data Protection Regulation (EU 2016/679) and follow strict internal rules to properly safeguard personal data against loss, theft and unauthorised access.

The collection, storage and use of Investors personal data are carried out for the specific, explicitly stated and legitimate purpose of rendering investment services as set out in the agreement between the Investment Manager Company (ACM) and its affiliated Schemes and between the Schemes and their Investors in compliance with the regulatory obligations and in the performance of a task carried out in the public interest. (e.g., to prevent or detect offences)

The collection of personal data may include:

- Identification data, e.g., names, addresses, telephone numbers, email addresses, business contact information;
- Personal characteristics, e.g., date of birth, country of birth;
- Professional information, e.g., employment and job history, title, representation authorities;
- Identifiers issued by public bodies, e.g., passport, identification card, TIN -Tax Identification Payer;
- Financial information, e.g. financial and credit history information, bank details.
- Transaction / investment data, e.g., current and past investments, investment profile, invested amount, number and value of shares held, transaction details;

More specifically, the collection and process of personal data is necessary for the performance of a contract to which Investors are a party, which includes the following Processing Operations:

- the opening and management of a shareholding account, including all related operations for Investor's identification;

- the processing of subscription, transfer and redemption requests in our affiliated Schemes, as well as for maintaining the ongoing relationship with respect to the holdings.

Also, personal data are collected and processed to comply with legal and regulatory obligations to which we are subject, including to:

- provide offering documentation about the Schemes;

- comply with regulatory obligations;

- carry out any other form of cooperation with, or reporting to, competent administrations, supervising authorities, law enforcement authorities and other public authorities (e.g., in the field of anti-money laundering and combating terrorism financing ("AML-CTF")), for the prevention and detection of crime under tax law (e.g., reporting of name, address, date of birth, tax identification number (TIN), account number and account balance to the tax authorities under the Common Reporting Standard ("CRS") or Foreign Account Tax Compliance Act ("FATCA") or other tax legislation to prevent tax evasion and fraud as applicable);

- prevent fraud, bribery, corruption and the provision of financial and other services to persons subject to economic or trade sanctions on an on-going basis in accordance with our AML-CTF procedures, as well as to retain AML-CTF and other required records for screening purposes;

Furthermore, we may process personal data in relation to legitimate interests we pursue in order to:

- develop our Business Relationship with you;

- improve our internal business organisation and operations;

- establish, exercise and/or defend actual or potential legal claims, investigations or similar proceedings;

The provision of personal data may be mandatory, e.g., in relation to our compliance with legal and regulatory obligations to which we are subject. Please be aware that not providing such information

may preclude us from pursuing a Business Relationship with, and/or from rendering our services to you.

To achieve the purpose of rendering an investment service, we collect or receive personal data:

- directly from the Investors through documentation directly sent to us; and/or
- indirectly from other external sources, including any publicly available sources (e.g., UN or EU sanctions lists), information available through subscription services (e.g., CDDS-Customer Due Diligence Solutions)

If necessary we reserve the right to disclose or make accessible the personal data to the following recipients, provided this is legally or otherwise authorised or required:

- public / governmental administrations, courts, competent authorities (e.g., financial supervisory authorities or tax authorities) ;
- auditors or legal advisors.

As from 25th May 2018, Subscription Forms will be duly updated to collect Investor(s)' consent to treat personal data according to GDPR' principles for the purpose of delivering the investment service requested (Due Diligence purposes, for communicating with shareholders for sending valuation statements and subscription/redemption contract notes, newsletters amongst others)

According to Offering Memorandum of the Schemes, Investor's Personal Data are transmitted to the Fund Administrator ("the Processor"). Such Personal Data are the original documents regarding the investments of the Investors (subscription forms, experienced/qualifying investor declaration forms and authenticated copies of passports amongst others).

Certified copies of these documents are in files at the Investment Manager Company (ACM) premises. Whenever possible, both hard copies and soft copies (scans) are stored for every client document received.

Amstel Capital (Malta) Ltd and its affiliated Schemes are responsible only for the processing of personal data as per this Privacy Policy and are not responsible for 3rd party's use of Investors' Personal data, where such use is permitted by the Authority and for their own purposes.

In case a data breach occurs, even when occurs to the Processor, and the breach poses a risk to an individual's rights and freedoms, we will notify the supervisory authority (Commissioner of Data Protection – Mr. Joseph Ebejer) without undue delay, and at the latest within 72 hours after having become aware of the breach.

You have the right, subject to GDPR legislation, to:

- request access to, and receive a copy of, the personal data we hold;

- if appropriate, request rectification or erasure of the personal data that are inaccurate;

- request the erasure of the personal data when the Processing is no longer necessary for the Purposes, or not or no longer lawful for other reasons, subject however to applicable retention periods (kindly note that the Authority mandatory requirement is to keep personal data for 5 years after the last transaction);

- complain in relation to the processing of personal data and, absent a satisfactory resolution of the matter, file a complaint in relation to the Processing of personal data with the relevant data protection supervisory authority.

Nevertheless we will continue the processing of Personal Data if is

(i) legally mandatory);

(ii) necessary for the performance of the existing business relationship;

(iii) necessary for the performance of a task carried out in the public interest; or

(iv) necessary for the purposes of the legitimate interests we follow, including the establishment, exercise or defence of legal claims.

We consider Cyber Security a strategic issue and a possible operational risk and to protect our data against cyber crime have installed antivirus protection programme, covering all programmes on the computers. Furthermore ACM has also various Firewalls on different levels for protection of data against outside perpetrators.

ACM, AACF and AGUF workflow documents and files are stored on a Stand-alone Network, which receives firmware automatic updated. Only ACM approved software may be used on Fund Manager Company owned computer and Network. This additional measure has been taken in order to decrease the risks of viruses that could be detrimental to ACM.

Access to the network is strictly given to employees and directors only through a password which is updated regularly.

All login data and information are passwords protected and are accessible by relevant employees only. Employees keep confidential any password or security codes entrusted to them.

All confidential correspondence regarding the investors is kept in a cupboard which is locked. Access to clients files is done on the principle “Need to know” by the relevant employee.

Access to ACM premises and office is possible only by using a personalised electronic card access. In addition every visitors need to be registered at the reception.