Solid Financial Services Ltd

GDPR POLICY

Version 1

Summary
This Policy sets out how the ***Solid Financial Services Ltd*** (the 'Company') processes the personal data that it holds in relation to employees, staff, third parties (collectively 'the staff') as well as in relation to its clients (the "data subjects"). It outlines the Company's responsibilities under data protection legislation and regulation, setting out how it will comply, and provides instruction for staff handling personal data.
Scope
The Policy applies to all members of staff employed by the Company, including directors, staff/associates, contractors and any interns who are carrying out work on behalf of the Company.

Date	07.06.2021
Date of publication	14.06.2021
Date of original publication	14.06.2021
Next review date	01.06.2023
Revision Frequency	2 years

Contents

1. Introduction

Solid Securities and Financial Services Ltd (the "Company") is a Cyprus Investment Firm (CIF) that was incorporated and is operating as a private, limited liability company, with registration number HE128405, having its registered office and head offices in Limassol, Cyprus ("Solid" or the "Company"). The Company is licensed by the Cyprus Securities and Exchange Commission with license number 065/06. If you have any questions, need clarifications or want more details about how we use your personal information, you can contact the Company's Data Protection Officer at tel. **+357 25363680** or email **dpo@solid.com.cy**

The Company is committed to protecting your privacy and handling your data in an open and transparent manner. The protection of individuals via the lawful, legitimate and responsible processing and use of their personal data is a fundamental human right. The Company respects the right of individuals to have control over their personal date and ensures it acts in full compliance with legislative and regulatory requirements at all times.

The EU General Data Protection Regulation 2016/679 (hereafter "GDPR"), governs how the Company collects and processes personal data. Solid shall comply with all requirements for personal data protection as described by the GDPR and shall use all reasonable endeavors to:

- ensure the safe-keeping of personal data of data subjects which shall include but not necessarily be limited to keeping such data in a commonly used and machine-readable format that allows transmission of such data to the data subject or to any entity the Client requests,

- implement appropriate technical and organisational measures in an effective way in order to meet the requirements of GDPR and protect your rights,

- hold and process only of data strictly necessary for the completion of Solid's obligations,

- limit the access to personal data only to those needed to carry out the processing,

- maintain the ability to act and to indeed act on your request to obtain from Solid confirmation as to whether or not personal data concerning you is being processed, where and for what purpose,

- maintain the ability to provide and indeed to provide a copy of your personal data in an electronic format upon your request and maintaining the ability to erase and indeed to erase personal data and cease further dissemination and processing of the data upon your request provided that the obligation to process and maintain data for certain period of time in accordance with applicable legislation is not violated and appropriate conditions are met.

- effectively inform you without any undue delay and, at any rate, not later than within 72 hours of any personal data breach as well as of any breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Solid shall have the right, without giving prior notice to you, to disclose or report such details or any other details and/or information which Solid may deem necessary in order to comply with the provisions of any applicable law or third party or regulatory or other competent authority having the right to demand such disclosure or to comply with any obligation of Solid to proceed with such disclosure to any third party.

2. Purpose of this Policy

This Policy sets out how the Company will process the personal data of its staff and clients. This Policy applies to all personal data that the Company processes regardless of the format or media on which the data are stored or who it relates to.

3. Scope of this policy

This Policy applies to all members of staff employed by the Company, directors, staff/associates, contractors, and any interns who are carrying out work on behalf of the Company (referred to herein as you/your) involving the handling of personal data.

You have a crucial role to play in ensuring that the Company maintains the trust and confidence of the individuals about whom the Company processes personal data (including its own staff), complying with the Company's legal obligations and protecting the Company's reputation. This Policy therefore sets out what the Company expects from you in this regard.

Compliance with this Policy and the related policies and procedures is mandatory. Any breach of this Policy and any related policies and procedures may result in disciplinary action.

All members of staff must read, understand and comply with this Policy when processing personal data in the course of performing their tasks and must observe and comply with all controls, practices, protocols and training to ensure such compliance.

The Management of the Company is responsible for overseeing the implementation and review of this Policy (and the related policies and procedures).

4. Data Protection Principles

The GDPR is based on a set of core principles that the Company must observe and comply with at all times from the moment that personal data are collected until the moment that personal data are archived, deleted or destroyed.

The Company must ensure that all personal data are:

1. Processed lawfully, fairly and in a transparent manner (Lawfulness, fairness and transparency)
2. Collected only for specified, explicit and legitimate purposes (Purpose limitation)
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is to be processed (Data minimisation)
4. Accurate and where necessary kept up to date (Accuracy).
5. Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed (Storage limitation).
6. Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (Security, integrity and confidentiality)

The Company is responsible for, and must be able to demonstrate compliance with, all of the above principles

5. Lawfulness, fairness and transparency

Lawfulness and fairness

In order to collect and process personal data for any specific purpose, Solid must always have a lawful basis for doing so.

Without a lawful basis for processing, such processing will be unlawful and unfair and may also have an adverse impact on the affected data subjects.

Processing personal data will only be lawful where at least one of the following lawful bases applies:

1. The data subject has given their **consent** for one or more specific purposes
2. The processing is necessary for the **performance of a contract** to which the data subject is a party (for instance a contract of employment with the Company)
3. To comply with the Company's **legal obligations**
4. To protect the **vital interests** of the data subject or another person (this will equate to a situation where the processing is necessary to protect the individual's life)
5. To perform tasks carried out in the public interest or the exercise of official authority

6. To pursue the Company's **legitimate interests** where those interests are not outweighed by the interests and rights of data subjects.

The Company must identify and document the lawful basis relied upon by it in relation to the processing of personal data for each specific purpose or group of related purposes.

Consent as a lawful basis for processing

There is no hierarchy between the lawful bases for processing above, of which a data subject's consent is only one. Consent may not be the most appropriate lawful basis depending on the circumstances.

In order for a data subject's consent to be valid and provide a lawful basis for processing, it must be:

- specific (not given in respect of multiple unrelated purposes)
- informed (explained in plain and accessible language)
- unambiguous and given by a clear affirmative action (meaning opt-in: silence, inactivity or pre-ticked boxes will not be sufficient)
- separate and unbundled from any other terms and conditions provided to the data subject
- freely and genuinely given (there must not be any imbalance in the relationship between the Company and the data subject and consent must not be a condition for the provision of any product or service)

A data subject must be able to withdraw their consent as easily as they gave it.

Once consent has been given, it will need to be updated where the Company wishes to process the personal data for a new purpose that is not compatible with the original purpose for which they were collected.

Unless the Company is able to rely on another lawful basis for processing, a higher standard of explicit consent (where there can be no doubt that consent has been obtained, for example a signed document or a Yes/No option accompanied by clear consent wording) will usually be required to process special categories of personal data, for automated decision-making and for transferring personal data outside of the EEA.

Where the Company needs to process special categories of personal data, it will generally rely on another lawful basis that does not require explicit consent; however, the Company must provide the data subject with a fair processing notice explaining such processing.

If the Company is unable to demonstrate that it has obtained consent in accordance with the above requirements, it will not be able to rely upon such consent.

Transparency

The concept of transparency requires the Company to ensure that any information provided by the Company to data subjects about how their personal data will be processed is concise, easily accessible, easy to understand and written in plain language.

Where the Company has not been transparent about how it processes personal data, this will call the lawfulness and fairness of the processing into question.

The Company can demonstrate transparency through providing data subjects with appropriate privacy notices or fair processing notices **before** it collects and processes their personal data and at appropriate times throughout the processing of their personal data.

The GDPR sets out a detailed list of information that must be contained in all privacy notices and fair processing notices, including:

- the types of personal data collected;
- the purposes for which they will be processed;
- the lawful basis relied upon for such processing (in the case of legitimate interests, the Company must explain what those interests are);
- the period for which they will be retained;
- who the Company may share the personal data with;
- and, if the Company intends to transfer personal data outside of the EEA, the mechanism relied upon for such transfer (see Transfers of personal data outside of the EEA).

Where the Company obtains any personal data about a data subject from a third party (for example, CVs from recruitment agents for potential employees it must check that it was collected by the third party in accordance with the GDPR's requirements and on a lawful basis where the sharing of the personal data with the Company was clearly explained to the data subject.

6. Purpose limitation

The Company must only collect and process personal data for specified, explicit and legitimate purposes that have been communicated to data subjects **before** the personal data have been collected.

The Company must ensure that it does not process any personal data obtained for one or more specific purposes for a new purpose that is not compatible with the original purpose. Where the Company intends to do so, it must inform the data subjects **before** using their personal data for the new purpose and, where the lawful basis relied upon for the original purpose was consent, obtain such consent again.

7. Data minimisation

The personal data that the Company collects and processes must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is to be processed.

You must only process personal data when necessary for the performance of your duties and tasks and not for any other purposes. Accessing personal data that you are not authorised to access, or that you have no reason to access, may result in disciplinary action and in certain circumstances, may constitute a criminal offence.

You may only collect personal data as required for the performance of your duties and tasks and should not ask a data subject to provide more personal data than is strictly necessary for the intended purposes.

You must ensure that when personal data are no longer needed for the specific purposes for which they were collected, that such personal data are deleted, destroyed or anonymised.

You must observe and comply with the Company's Records Management, Retention Policy and Records Retention Schedule.

8. Accuracy

The personal data that the Company collects and processes must be accurate and, where necessary, kept up-to-date and must be corrected or deleted without delay when the Company discovers, or is notified, that the data are inaccurate.

You must ensure that you update all relevant records if you become aware that any personal data are inaccurate. Where appropriate, any inaccurate or out-of-date records should be deleted or destroyed.

9. Storage limitation

The personal data that the Company collects and processes must not be kept in a form that identifies a data subject for longer than is necessary in relation to the purposes for which it was collected (except in order to comply with any legal, accounting or reporting requirements).

Storing personal data for longer than necessary may increase the severity of a data breach and may also lead to increased costs associated with such storage.

The Company will maintain policies and procedures to ensure that personal data are deleted, destroyed or anonymised after a reasonable period of time following expiry of the purposes for which they were collected.

You must regularly review any personal data processed by you in the performance of your duties and tasks to assess whether the purposes for which the data were collected have expired.

Where appropriate, you must take all reasonable steps to delete or destroy any personal data that the Company no longer requires in accordance with the Company's Records Management Policies.

All privacy notices must inform data subjects of the period for which their personal data will be stored or how such period will be determined.

You must observe and comply with the Company's Records Management and Retention Policy and Records Retention Schedule.

10. Security, integrity and confidentiality

Security of personal data

The personal data that the Company collects and processes must be secured by appropriate technical and organisational measures against accidental loss, destruction or damage, and against unauthorised or unlawful processing.

The Company will develop, implement and maintain appropriate technical and organisational measures for the processing of personal data taking into account the:

• nature, scope, context and purposes for such processing
• volume of personal data processed
• likelihood and severity of the risks of such processing for the rights of data subjects

The Company will regularly evaluate and test the effectiveness of such measures to ensure that they are adequate and effective.

You are responsible for ensuring the security of the personal data processed by you in the performance of your duties and tasks.

You must ensure that you follow all procedures that the Company has put in place to maintain the security of personal data from collection to destruction.

You must ensure that the confidentiality, integrity and availability of personal data are maintained at all times:

• **Confidentiality:** means that only people who need to know and are authorised to process any personal data can access it
• **Integrity:** means that personal data must be accurate and suitable for the intended purposes
• **Availability:** means that those who need to access the personal data for authorised purposes are able to do so.

You must not attempt to circumvent any administrative, physical or technical measures the Company has implemented as doing so may result in disciplinary action and in certain circumstances, may constitute a criminal offence.

Reporting personal data breaches

What is a Data Breach

A personal data breach is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, whether by accidental or deliberate causes".

The General Data Protection Regulation (GDPR) introduces a duty on all organisations to report certain types of personal data breach to the relevant authority.

Personal data breaches can include the following:

- access to personal data by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- hand-held devices / laptops containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data

Practical examples of breaches I should report to the Data Protection Officer (DPO)

- I have lost a USB stick which holds personal information
- My work laptop has been stolen (from work or elsewhere)
- I sent a data file to a different person from the intended recipient
- I sent a letter including someone's bank details to an incorrect address
- I printed a document which contained personal data, left it on my desk and I cannot locate it.

Examples of personal and sensitive personal data:

Personal Data

- Full Name
- Date of Birth
- Address
- Postcode
- Telephone Numbers
- Email Address
- Employee/Client ID Number
- Passport Number
- Bank Details

Sensitive Data

- Racial or ethnic origin of the data subject
- Political Opinions Address
- Religious beliefs or beliefs of a similar nature
- Physical, mental or health condition
- Any proceeding of any committed or alleged commission of any offence
- Biometric Data (i.e.: fingerprints, facial recognition)

It is the responsibility of everyone at Solid to ensure they keep personal data safe. In the event that you are aware of a security breach, you must ensure that you observe and comply with the Company's personal data breach procedure described below.

If you believe you may have encountered a data breach, you must report it using the form in Appendix 1 and send this to the DPO at: dpo@solid.com.cy

Personal Data Procedure

1) A member of staff is aware of or is made aware of an incident and identifies personal data is involved
2) The staff member completes the data breach form and provide it to the DPO.
3) An assessment is made by the DPO and a decision is made as to whether the breach will result in a risk to individuals' rights and freedoms. All data security breaches will be managed according to risk. After the identification of the breach, the risks associated with the breach will be assessed in order to identify an appropriate response. Appendix 1 should be used to identify the exact nature of the breach and the severity; this information can then be used to establish the action required. The investigation will take into account:
   a) the type of data involved and its sensitivity
   b) the protections which are in place (e.g. encryption)
   c) What has happened to the data, has it been lost or stolen
   d) whether the data could be put to any illegal or inappropriate use
   e) who the individuals are, number of individuals involved and the potential effects on those data subject(s)
   f) whether there are wider consequences to the breach

In case DPO decides that the breach does not result in a risk to individuals' rights and freedom there will be no need to report the incident to the Commissioner for personal data protection.

4) However, if the breach results in a risk to individual's rights and freedoms the DPO must Report it to the Commissioner for personal data protection. The GDPR introduces the obligation to notify data breaches to the Commissioner for of Personal Data Protection, without undue delay and, where feasible, not later than 72 hours after having become aware of it (article 33). Certain exceptions may apply in accordance with article 33 of the GDPR. The relevant reporting form can be found on the website of the Office of the Commissioner for Personal Data Protection at the following address:

http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/6AC026346F0A7274C22582600037F9DF/$file/Data breach notification form GDPR ENG v3.xlsx

For cross-border cases, the data breach should be notified to the lead supervisory authority in accordance with Article 55.

When the data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller must also communicate the data breach to the data subject without undue delay.

Data Subject Notification

When a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, we will always communicate the personal data breach to the data subject without undue delay, in a written, clear and legible format.

Notification to the individual(s) whose personal data has been affected by the incident will include a factual description of how and when the breach occurred and the data involved, along with actions taken by the Company. Individuals will also be provided with the name and contact details of the DPO for further information.

More specifically, the notification to the Data Subject shall include:

• The nature of the personal data breach
• The name and contact details of our Data Protection Officer and/or any other relevant point of contact (for obtaining further information)
• A description of the likely consequences of the personal data breach
• A description of the measures taken or proposed to be taken to address the personal data breach (including measures to mitigate its possible adverse effects)

We reserve the right not to inform the data subject of any personal data breach where we have implemented the appropriate technical and organisational protection measures which render the data unintelligible to any person who is not authorised to access it (i.e. encryption, data masking etc) or where we have taken subsequent measures which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise. If informing the data subject of the breach involves disproportionate effort, we reserve the right to instead make a public communication whereby the data subject(s) are informed in an equally effective manner.

However, there will be no need to notify the individuals affected in case the data breach is likely to result in a low risk to the rights and freedoms of natural persons.

In any case, the breach must be recorded on the incidents and breaches log. All records and notes taking during the identification, assessment and investigation of the data breach are recorded and authorised by the Data Protection Officer and are retained for a period of 6 years from the date of the incident. Incident forms are to be reviewed monthly to assess for patterns or breach reoccurrences and actions taken to prevent further incidents from occurring

Failure to report a breach to the Commissioner may result to a sanction imposed to the Company by the Commissioner, including a fine. It may also constitute an offence according to the provisions of article 33 of the Law providing for the Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of such Data (Law 2018125(I)/2018).

The Company has put in place appropriate procedures to deal with any personal data breach and will notify the Commissioner for Personal Data Protection and/or data subjects where the Company is legally required to do so.

If you know or suspect that a personal data breach has occurred, you must contact the Data Protection Officer, and IT Services if relevant, immediately to report it and obtain advice, and take all appropriate steps to preserve evidence relating to the breach and follow the Company's personal data breach procedure described above.

11. Sharing personal data

You are not permitted to share personal data with third parties unless the Company has agreed to this in advance, this has been communicated to the data subject in a privacy notice or fair processing notice beforehand and, where such third party is processing the personal data on our behalf, the Company has undertaken appropriate due diligence of such processor and entered into an agreement with the processor that complies with the GDPR's requirements for such agreements. The Company does not use another organization in order to obtain assistance with the processing of personal data. However, in the event that the Company decides to establish such a business relationship with another organization, a written contract will govern such a relationship.

The transfer of any personal data to an unauthorised third party would constitute a breach of the Lawfulness, fairness and transparency principle and, where caused by a security breach, would constitute a personal data breach.

Do not share any personal data with third parties, including the use of freely available online and cloud services for work-related purposes, unless you are certain that the conditions outlined above apply. Seek advice from the Data Protection Officer, or IT Manager, if you are unsure.

12. Transfers outside of the European Economic Area (EEA)

The GDPR prohibits the transfer of personal data outside of the EEA in most circumstances in order to ensure that personal data are not transferred to a country that does not provide the same level of protection for the rights of data subjects. In this context, a "transfer" of personal data includes transmitting, sending, viewing or accessing personal data in or to a different country.
The Company may only transfer personal data outside of the EEA if one of the following conditions applies:
• the European Commission has issued an "adequacy decision" confirming that the country to which we propose transferring the personal data ensures an adequate level of protection for the rights and freedoms of data subjects (this applies to only a small number of countries)

• appropriate safeguards are in place, such as binding corporate rules, standard contractual clauses that have been approved by the European Commission, an approved code of conduct or certification mechanism which, in each case, can be obtained from the Data Protection Officer

• the data subject has given their explicit consent to the proposed transfer, having been fully informed of any potential risks

• the transfer is necessary in order to perform a contract between the Company and a data subject, for reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the data subject in circumstances where the data subject is incapable of giving consent

• the transfer is necessary, in limited circumstances, for the Company's legitimate interests

You must ensure that you do not transfer any personal data outside of the EEA except in the circumstances set out above and provided that the Company has agreed to this in advance.

13. Data subject rights and requests

The GDPR provides data subjects with a number of rights in relation to their personal data. These include:

Right to withdraw consent: where the lawful basis relied upon by the Company is the data subject's consent, the right to withdraw such consent at any time without having to explain why

• **Right to be informed**: the right to be provided with certain information about how we collect and process the data subject's personal data (see Transparency)

• **Right of subject access**: the right to receive a copy of the personal data that we hold, including certain information about how the Company has processed the data subject's personal data

• **Right to rectification**: the right to have inaccurate personal data corrected or incomplete dated completed

• **Right to erasure (right to be forgotten):** the right to ask the Company to delete or destroy the data subject's personal data if: the personal data are no longer necessary in relation to the purposes for which they were collected; the data subject has withdrawn their consent (where relevant); the data subject has objected to the processing; the processing was unlawful; the personal data have to be deleted to comply with a legal obligation; the personal data were collected from a data subject under the age of 13, and they have reached the age of 13.

• **Right to restrict processing:** the right to ask the Company to restrict processing if: the data subject believes the personal data are inaccurate; the processing was unlawful and the data subject prefers restriction of processing over erasure; the personal data are no longer necessary in relation to the purposes for which they were collected but they are required to establish, exercise or defend a legal claim; the data subject has objected to the processing pending confirmation of whether the Company's legitimate interests grounds for processing override those of the data subject

• **Right to data portability:** in limited circumstances, the right to receive or ask the Company to transfer to a third party, a copy of the data subject's personal data in a structured, commonly-used machine-readable format

• **Right to object:** the right to object to processing where the lawful basis for processing communicated to the data subject was the Company's legitimate interests and the data subject contests those interests

• **Right to object to direct marketing:** the right to request that we do not process the data subject's personal data for direct marketing purposes

• **Right to object to decisions based solely on automated processing (including profiling):** the right to object to decisions creating legal effects or significantly affecting the data subject which were made solely by automated means, including profiling, and the right to request human intervention

• **Right to be notified of a personal data breach:** the right to be notified of a personal data breach which is likely to result in a high risk to the data subject's rights or freedoms

• **Right to complain:** the right to make a complaint to the Office of the Commissioner for Personal Data Protection or another appropriate supervisory authority

You must be able to identify when a request has been made and must verify the identity of the individual making a request before complying with it. You should be wary of third parties deceiving you into providing personal data relating to a data subject without their authorisation.

For more information in relation to the employees' rights, please refer to the Employee Policy below. In relation to clients' rights please see attached the **Privacy Statement** of the Company, also available on the Company's website at: www.solid.com.cy

14. Accountability and record-keeping

The Company is responsible for and must be able to demonstrate compliance with the data protection principles and the Company's other obligations under the GDPR. This is known as the 'accountability principle'.

The Company must ensure that it has adequate resources, systems and processes in place to demonstrate compliance with the Company's obligations including:

• appointing a suitably qualified and experienced Data Protection Officer (DPO) and providing them with adequate support and resource

• ensuring that at the time of deciding how the Company will process personal data, and throughout its processing, implementing appropriate technical and organisational measures that are designed to ensure compliance with the data protection principles (known as 'Data Protection by Design').

This means that companies/organisations are encouraged to implement technical and organisational measures, at the earliest stages of the design of the processing operations, in such a way that safeguards privacy and data protection principles right from the start.

• ensuring that, by default, only personal data that are necessary for each specific purpose are processed both in relation to the nature, extent and volume of such personal data, the period of storage and the accessibility of the personal data (known as 'Data Protection by Default').

• ensuring that where any intended processing presents a high risk to the rights and freedoms of data subjects, the Company has carried out an assessment of those risks and is taking steps to mitigate those risks, by undertaking a 'Data Protection Impact Assessment'.

• integrating data protection into the Company's internal documents, privacy policies and fair processing notices

• regularly training the Company's staff on the GDPR, this policy and the Company's related policies and procedures, and maintaining a record of training completion by members of staff

• regularly testing the measures implemented by the Company and conducting periodic reviews to assess the adequacy and effectiveness of this policy, and the Company's Related policies and procedures

The Company must keep full and accurate records of all its processing activities in accordance with the GDPR's requirements.

You must ensure that you have undertaken the necessary training providing by the Company and, where you are responsible for other members of staff, that they have done so.

You must further review all the systems and processes under your control to ensure that they are adequate and effective for the purposes of facilitating compliance with the Company's obligations under this policy.

You must ensure that you observe and comply with all policies and guidance in relation to GDPR.

15. Changes to this policy

The Company may make amendments to this policy at any time without notice, so please ensure you view the latest version.

EMPLOYEE PRIVACY NOTICE

Your privacy notice is important to us, and we are committed to the protection of your privacy in your employment with us. This Privacy Policy describes what Personal Data our Company collects about you as a prior, current or former employee (the "Employee").

Personal Data means information that we obtain from you in connection with your current or past employment with us that can identify you.

This Privacy Policy covers what Personal Data we collect about you, how the Personal Data will be used and shared (if at all), how the Personal Data will be stored, and your rights in relation to the collection of your Personal Data during, before, or after the employment with the Company. It also describes your rights in relation to your Personal Data and how your Personal Data is handled by our third-party data processors.

Scope of the Employee Privacy Notice

This Privacy Notice applies to the Personal Data of all individuals who are or were employed by the Company. These individuals shall be referred as Employee or Employees.

Why do we collect your personal information

We process your personal information to meet our legal, statutory and contractual obligations and to enable us to recruit, employ and train you in the course of your employment with us. We will never collect any unnecessary personal data from you and do not process your information in any way, other than as specified in this notice.

Collection of Personal Data:

We collect different types of Personal Data in different ways. In order to ensure that we are meeting our responsibilities as your employer, we collect, process and maintain different types of Personal Data in relation to the individuals that are or were employed by us, including but not limited to:

- Name
- Gender
- Date of Birth
- Home Address
- Personal Email
- Financial Information (social insurance number, bank account information)
- Forms that contain information in relation to health care plans, insurance policies and the like.
- Home Telephone Number
- Mobile Telephone Number
- Contact information of the individual that you list to be the first notified in the event of an emergency (i.e: phone number and any other personally identifying
- Professional References

- Information about your entitlement to work in Cyprus.
- In certain cases, Special Category Data (i.e., health/medical information)

How We Use Your Personal Data

Solid takes your privacy very seriously and will never disclose, share or sell your data without your consent; unless required to do so by law.

We only retain your data for as long as is necessary and for the purpose(s) specified in this notice. The purposes and reasons for processing your personal data are detailed below:

• We process your personal data in the performance of a contract as your employer, to ensure that we meet our legal employer obligations and the requirements of employment law

• We process your personal data as part of our legal obligation for business accounting, payroll and tax purposes

• We process special category data about you as part of our employment obligations, to ensure that any disabilities and health conditions are known.

Your Rights

You have the right to access any personal information that Solid processes about you and to request information about:

- What personal data we hold about you
- The purposes of the processing
- The categories of personal data concerned
- The recipients to whom the personal data has/will be disclosed
- How long we intend to store your personal data for
- If we did not collect the data directly from you, information about the source
- If you believe that we hold any incomplete or inaccurate data about you, you have the right to ask us to correct and/or complete the information and we will strive to do so as quickly as possible; unless there is a valid reason for not doing so, at which point you will be notified.
- You also have the right to request erasure of your personal data or to restrict processing in accordance with the data protection laws.

Sharing and Disclosing Your Personal Information

We do not share or disclose any of your personal information without your consent, other than for the purposes specified in this notice or where there is a legal requirement.

Safeguarding Measures

Solid takes your privacy seriously and takes every reasonable measure and precaution to protect and secure your personal data. We work hard to protect you and your information from unauthorised access, alteration, disclosure or destruction and have several layers of security measures in place.

Transfers Outside the EU

Personal data in the European Union is protected by the General Data Protection Regulation (GDPR) but some other countries may not necessarily have the same high standard of protection for your personal data. Solid does not transfer or store any personal data outside the EU.

Consequences of Not Providing Your Data

You are not obligated to provide your personal information to Solid, however, as this information is required for us to employ you, we will not be able to offer employment without certain personal information.

How Long We Keep Your Data

Solid only ever retains personal information for as long as is necessary and we have strict review and retention policies in place to meet these obligations. For more information you may refer to the Data Retention Policy below.

Special Categories Data

As your employer, we have a legitimate interest and, in some cases, a legal obligation to process certain special category data about you.

This can include but is not limited to information about health conditions. Where we collect such information, we do so under the GDPR's Article 9(2)b according to which:

"processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

We will only request and process the minimum necessary for the specified purpose and ensure that the required protective measures and security is placed on all special category data.

Lodging A Complaint

Solid only processes your personal information in compliance with this privacy notice and in accordance with the relevant data protection laws. If, however you wish to raise a complaint regarding the processing of your personal data or are unsatisfied with how we have handled your information please contact our Data Protection Officer at: dpo@Solid.com.cy

Modifications and Revisions

We reserve the right to modify, revise or otherwise amend this Privacy Policy at any time and in any manner without your consent.

DATA RETENTION POLICY

1. Purpose

The purpose of this Policy is to ensure that necessary records and documents of the Company are adequately protected and maintained and to ensure that records that are no longer needed by the Company or are of no value are discarded at the proper time. This Policy is also for the purpose of aiding employees of the Company in understanding their obligations in retaining electronic documents – including e-mail, Web files, text files, sound and video files, PDF documents, and all Microsoft Office or other formatted files.

2. Policy

This Policy represents the Company's policy regarding the retention and disposal of records and the retention and disposal of electronic documents.

3. Record Retention Schedule

A Record Retention Schedule has been prepared by the Company that is approved as the initial maintenance, retention and disposal schedule for physical records of the Company and the retention and disposal of electronic documents. The Data Protection Officer defines the time period for which the documents and electronic records should be retained through the Data Retention Schedule. We will make modifications to the Record Retention Schedule from time to time to ensure that it includes the appropriate document and record categories for the Company; monitor legislation affecting record retention; annually review the record retention and disposal program; and monitor compliance with this Policy.

In addition, any retained information can only be used for the purpose for which it is stored. This is compliant with the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).

4. Retention Periods

As required by law, the Company shall not retain any personal data for any longer than is necessary in light of the purpose(s) for which that data is collected.

The required retention period will be deemed to be 3 years from the date of creation of the document, unless otherwise mandated differently by applicable law.

For instance:

According to article 68 of the AML Law No. 188(I)2007 (the "AML Law"), a Cypriot Investment Firm must maintain the following documents and information, for a period of five (5) years after the end of the business relationship with the customer or after the date of an occasional transaction:

(a) Copies of documents and information required for compliance with the customer due diligence requirements as determined in the present Law;

(b) relevant evidence and records of transactions which are necessary for the identification of transactions;

(c) relevant correspondence documents with customers and other persons with whom a business relationship is maintained

Similarly, under MiFID II, when a CIF executes client orders and makes decisions to enter into transactions, it is required to keep records for at least five years immediately after receiving a client order or making a decision to deal in relation to every initial order received and every initial decision to deal.

Investment firms are also required to keep records of:

- the content and timing of instructions received from clients
- allocation decisions taken for each operation in relation to underwriting or placing of orders so as to retain a complete audit trail between the movements registered in clients' accounts and the instructions received by and decisions taken by the investment firm.

These records must be retained for five years.

Records must also be retained by firms in relation to any client money that is held on behalf of clients. These records must be sufficient to determine the amount of client money the firm holds for each of its clients and to show and explain the firm's transactions and commitments for the client money it holds. These records must be retained for a period of five years from the later of the date they were created or the date they were last modified.

Therefore, if a regulated firm has a legal obligation under a specific legislation to hold records for a specified period of time, this legal obligation will prevail over a request for erasure of those records before the period prescribed by the specific legislation has expired.

5. Suspension of Record Disposal In Event of Legal Proceedings or Claims

There are certain occasions when information needs to be preserved beyond any limits set out in the Policy. The Policy must be SUSPENDED relating to a specific customer or document and the information retained beyond the period specified in the Company’s Data Retention Schedule in the following circumstances:

- Legal proceedings or a regulatory or similar investigation or obligation to produce information are known to be likely, threatened or actual.
- A crime is suspected or detected.
- Information is relevant to a company in liquidation or receivership, where a debt is due to the Company.

- Information is considered by the owning department to be of potential historical importance and this has been confirmed by the DPO.
- In the case of possible or actual legal proceedings, investigations or crimes occurring, the type of information that needs to be retained relates to any that will help or harm the Company or the other side's case or liability or amount involved.
- If there is any doubt over whether legal proceedings, an investigation or a crime could occur, or what information is relevant or material in these circumstances, the DPO should be contacted and legal advice should be sought.

The DPO shall take such steps as is necessary to promptly inform all staff of any suspension in the further disposal of documents.

6. Destruction of Data

The Company and its employees should therefore, on a regular basis, review all data, whether held electronically on their device or on paper, to decide whether to destroy or delete any data once the purpose for which those documents were created is no longer relevant.

Once the decision is made to dispose according to the Retention Schedule, the data should be deleted, shredded or otherwise destroyed to a degree equivalent to their value to others and their level of confidentiality. The method of disposal varies and is dependent upon the nature of the document.

For example, any documents that contain sensitive or confidential information (and particularly sensitive personal data) must be disposed of as confidential waste and be subject to secure electronic deletion. In this context, the employee shall perform the tasks and assume the responsibilities relevant for the information destruction in an appropriate way. The specific deletion or destruction process may be carried out by an employee and must first inform the DPO The Data Protection Officer shall fully document and approve the destruction process.

7. Security of personal information

The Company will take reasonable technical and organisational precautions to prevent the loss, misuse or alteration of your personal information.

The Company will store all personal information on our secure (password- and firewall-protected) servers.

The Client should acknowledge that the transmission of information over the internet is inherently insecure, and that the Company cannot guarantee the security of data sent over the internet.

The Client will be responsible for keeping their Username and Password used for accessing the Company's website confidential; The Company will not ask for password other than when needed to log in to our website.

8. Amendments

The Company may update this policy from time to time by publishing a new version. This page should be checked occasionally to ensure that the policy remains relevant.

9. Applicability

This Policy applies to all physical records generated during the Company's operation, including both original documents and reproductions. It also applies to the electronic documents described above.

APPENDIX 1

OFFICE USE ONLY	
Date received	
Received by	
Breach ref number	

Personal Data Breach Notification Form

Please see the Company's Personal Data Breach Procedure which relates to this form. This form should be used to report any actual, suspected, threatened or potential personal data breach in accordance with such procedure.

This form should be completed as fully as possible based on currently available information.

If you have any questions regarding the completion of this form, please contact the DPO of the Company via email at dpo@Solid.com.cy

Information about you	
Name	
Job title	
Email address	
Phone number	

Note: We will get in touch with you if we require any further information or as part of our investigations relating to the breach.

Information about the personal data breach				
Date/time breach occurred	**Date**		**Time**	
Date/time breach identified	**Date**		**Time**	
Is the breach ongoing?	☐	Yes		
	☐	No		
	☐	Unsure		
Primary cause of breach	☐	Malicious attack		
	☐	Accident (e.g. system failure)		

	☐	Negligence (e.g. human error)
	☐	Other (see description below)
Description of events giving rise to the breach (include details such as timings, the resources affected or involved in the breach and any individuals that have been notified)		
Description of personal data accessed, altered, destroyed, disclosed or lost (include details such as the categories of personal data affected, volume of records affected)		
Categories of individuals affected	☐	Clients
	☐	Staff
	☐	Other:
Number of individuals affected		
Description of any action(s) taken to date		