Data Subject Access Request Policy

If your personal data is held by Astrala Advisory Services, you have the right to ask the Data Controller for the following:

- **Confirmation:** Whether they are currently processing any of your information.
- **Details:** A clear description of the data they have and why they are using it.
- **Sharing:** A list of any organisations that have received or might receive your data.
- **Origin:** Information on where they originally obtained your data (if available).
- **Copies:** A physical or digital copy of the actual information they hold about you.

How to Request Your Data

A formal application for your personal information is called a **Subject Access Request (SAR)**. However, not every inquiry needs to be treated as a formal legal request.

The text of the GDPR is available in all EU languages on the European Commission website and in pdf format in English by clicking here.

Routine vs. Formal Requests

If your request covers information we provide during our regular operations, such as a bank customer asking for a routine statement, Astrala Advisory Services may handle it as a "business-as-usual" matter rather than a formal SAR.

Making a Valid Request

- **Clear Statement of Request:** Explicitly state that you are making a "Subject Access Request" or "Data Subject Access Request" to access your personal data.
- **Your Personal Details:** Full name, current address, and any previous addresses from the last 6 years (if relevant).
- **Verification of Identity:** Enough proof to confirm you are who you say you are. This may include a copy of your passport, driving license, or utility bill, especially if your identity is not obvious (e.g., if you are a former employee or customer).
- **Specific Information Requested:** Please be as targeted as possible e.g. (You may wish to specify departments such as HR or Marketing), time periods, or types of data (e.g., emails, files) which would help us find your information faster.
- **Contact Information:** The best way to reach you, such as your email address.

What Happens Next?

Once you submit your request, the Data Controller will provide you with a **Privacy Notice** explaining your rights and how your data is processed.

The one-month response deadline begins when we are in receipt of the request. While Astrala Advisory Services aims to respond as quickly as possible, we will ensure a full response within this one-month window.

Direct Communication with You

Once we receive a valid Subject Access Request (SAR), Astrala Advisory Services will contact you directly to manage your request.

Clarifying Your Request: We may reach out to help you narrow down the specific information you need. We can "stop the clock" on the one-month response period while we wait for you to clarify a large or complex request. Pinpointing exact dates or departments helps us provide your data faster and more efficiently.

Comprehensive Searches: While focusing your request saves time for everyone, we respect your right to access all your data. If you confirm that you require a copy of everything we hold, we will conduct a full and exhaustive search across all our digital and manual records.

Reasonable and Proportionate Effort: We are committed to finding your information using "reasonable and proportionate" search methods. We will provide this data in a clear, accessible format while ensuring the privacy of other individuals is protected.

Our Search Process

To ensure we find all your information, Astrala Advisory Services follows a structured internal search process:

Comprehensive Search: Unless we have agreed with you to narrow the request's scope, we will search all relevant digital databases and manual filing systems across the entire organisation to comply with **Cyprus GDPR.**

Active Data Focus: We are not required to search back-up files, as these are simply copies of data already held in our "active" or archived systems.

Centralised Coordination: To ensure accuracy, one dedicated person manages the entire response. They are responsible for requesting information from every department and gathering all results.

Collating Results: The coordinator will organise all findings into two primary sets of records:

Digital Records: A printout of all relevant computerised information.

Physical Records: Copies of all relevant manual files.

This centralised approach ensures that the information we provide is as complete and organised as possible before it is sent to you

Handling Manual Files

Manual (paper) files are subject to the **Cyprus GDPR** if they meet the legal definition of a "relevant filing system."

The main test is whether the records are part of a highly structured set. This means the files must be organised in a way that allows specific information about an individual to be easily found.

Examples of Structured Sets:

- Files stored in alphabetical order by name.
- Records organised by payroll or identification numbers.
- If a manual file is part of such a system, it is considered personal data and must be included in our search.

Handling Data After a Request is Received

Receiving a Subject Access Request (SAR) should not disrupt the day-to-day operations of the Data Controller. However, specific rules apply to the data being requested:

No Alterations: Once a valid request is received, we are not permitted to change, delete, or "clean up" the information.

"As-Is" Records: The individual is entitled to see the information exactly as it exists in our systems at the time of the request. Even if the data is known to be inaccurate or out of date, it must be provided in its original form.

Corrections: Any necessary corrections or updates should only be handled after the request has been fulfilled, through the separate "Right to Rectification."

Protecting Third-Party Privacy

Once all data has been gathered, the coordinator must review the records to protect the privacy rights of other individuals.

Assessment of Third-Party Data: The coordinator will review every page from your perspective to identify if any information reveals another person's identity.

Known vs. Unknown Entities: If a third party is already known to you in that specific context, their information may be included. If their identity is not known, the coordinator will determine if the third-party information is necessary for the request or if it can be removed.

Redaction Process: To protect others, we will remove or "black out" (redact) names, contact details, or any other identifying markers.

Reasonable Disclosure: Our goal is to provide as much of your information as possible. If identifying details can be effectively obscured with a permanent marker or digital redaction tool, the rest of the content on that page will be included in your response.

General Exemptions and Legal Obligations

Certain types of information may be withheld from a Subject Access Request (SAR) based on legal exemptions under the **Cyprus GDPR** and the **EU GDPR Article 12(3).**

Ongoing Negotiations: We are not required to disclose information that would likely harm (prejudice) active negotiations between you and Astrala Advisory Services. Once these negotiations are finalised, the related files typically become accessible in the standard way.

Broad Digital Scope: Requests naturally include emails, archived data, CCTV footage, and recorded phone calls. We will search these areas if you specifically request them.

Security and Legal Action: We may withhold data if disclosure would compromise **national security**, interfere with the **prevention or detection of crime**, or hinder the **prosecution of offenders**.

Health Information: If your data contains medical records, we have a legal duty to consult a healthcare professional before release. This ensures that the disclosure will not cause serious harm or distress to you or others. **Note:** This consultation is not required if you have already seen the data or if you originally provided it to us yourself.

Compliance and Complaints: Failure to respond within the **one-month statutory deadline** is a breach of the Cyprus GDPR.

Under the **EU GDPR Article 12(3),** we may "stop the clock" on this deadline if we need you to clarify a large or complex request.

If you are unsatisfied with our response, you have the right to complain directly to the Commissioner for Personal Data Protection in Cyprus using Form “A”.