

Privacy Policy (May 2018)

1. Introduction

Apsiz Services Limited (Apsiz) is registered in England under Company Registration Number 8522031, and the Registered Office is Oak Bank, Oak Bank Lane, Hoole Village, Chester, Cheshire, CH2 4ER. Apsiz needs to collect and use certain types of information about the Individuals / Service Users who come into contact with our company in order to carry on our work which relates to any of the 3 key offerings at Apsiz (Procurement Consultancy, Bid Management Consultancy and Recruitment Support). This personal information must be collected and dealt with appropriately whether it's collected on paper, stored in a computer database, or recorded on other material and there are safeguards to ensure this under the Data Protection Act (DPA) 1998, and also the requirements of the General Data Protection Regulation (GDPR) 2018.

2. Data Controller

Apsiz is the Data Controller under the Act, which means that we determine what purposes personal information held will be used for. It is also responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for.

3. Disclosure

Apsiz may share data with other agencies such as the local authority, funding bodies and other voluntary agencies with given permission from the original data source, who can opt in or out at any time. The Individual / Service User will be made aware, in most circumstances, how and with whom their information will be shared. There are circumstances where the law allows Apsiz to disclose data (including sensitive data) without the data subject's consent. These are:

- Carrying out a legal duty or as authorised by the Secretary of State (i.e. a Cabinet Minister)
- Protecting vital interests of an Individual / Service User or other person
- The Individual / Service User has already made the information public
- Conducting any legal proceedings, obtaining legal advice or defending any legal rights
- Monitoring for equal opportunities purposes – i.e. race, disability or religion
- Providing a confidential service where the Individual / Service User's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill Individuals / Service Users to provide consent signatures.

Apsiz regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we engage with. Apsiz intends to ensure that personal information is treated lawfully and correctly. To this end, Apsiz will adhere to the Principles of Data Protection, as detailed in the Data Protection Act 1998 and also the requirements of the General Data Protection Regulation (GDPR) 2018. Specifically, the Principles require that personal information:

- Shall be processed fairly and lawfully and shall not be processed unless specific conditions are met,
- Shall be obtained only for one or more of the purposes specified in the Act, and shall not be processed in any manner incompatible with that purpose or those purposes,
- Shall be adequate, relevant and not excessive in relation to those purpose(s)
- Shall be accurate and, where necessary, kept up to date,
- Shall not be kept for longer than is necessary
- Shall be processed in accordance with the rights of data subjects under the Act,
- Shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information,
- Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory

ensures an adequate level of protection for the rights and freedoms of Individuals/Service Users in relation to the processing of personal information.

Apsiz will, through appropriate management and strict application of criteria and controls:

- Observe fully conditions regarding the fair collection and use of information
- Meet its legal obligations to specify the purposes for which information is used
- Collect and process appropriate information, and only to the extent that it is needed to fulfill its operational needs or to comply with any legal requirements
- Ensure the quality of information used
- Ensure that the rights of people about whom information is held, can be fully exercised under the Act. These rights include:
 - Right to be Informed – this is the right to transparency and therefore we are responsible to communicate with you what data we are collecting, storing / processing and how we intend to use it.
 - Right to Access – this is the right for Apsiz to confirm to individuals that we're processing your data and can give you access to this data if required.
 - Right to Rectification – this is the right for Apsiz to rectify any personal data that is inaccurate or incomplete. We have 1 month from the initial request to comply and any data previously disclosed with others must be notified of the changes.
 - Right to Erasure – this right is also known as the right to be forgotten. As an Individual / Service User you have the right to request to Apsiz for all of your information to be deleted.
 - Right to Restrict Processing – this right requires Apsiz to halt the use of any personal data on an Individual / Service user that is believed to be inaccurate. Until the issue is resolved we are able to store your data should this be required.
 - Right to Data Portability – this right allows any Individual / Service User to request, obtain and reuse their personal data. Such information can be provided to you in i.e. a CSV file or secure zip folder.
 - Right to Object – this right allows the Individual / Service User to object to the use of their data for direct marketing i.e. email marketing. If an Individual / Service User objects we must cease using any personal data for such activities.
- Take appropriate technical and organisational security measures to safeguard personal information
- Ensure that personal information is not transferred abroad without suitable safeguards
- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information
- Set out clear procedures for responding to requests for information

4. Data Collection

Informed consent is when an Individual / Service User clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data and then gives their consent. Apsiz will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form. When collecting data, Apsiz will ensure that the Individual / Service User:

- Clearly understands why the information is needed
- Understands what it will be used for and what the consequences are should the Individual / Service User decide not to give consent to processing
- As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed
- Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress

Privacy Policy (May 2018)

- e) Has received sufficient information on why their data is needed and how it will be used

5. Data Storage

Information and records relating to Individuals / Services Users will be stored securely and will only be accessible to authorised staff. Information will be stored for as long as it is needed or required statute and will be disposed of appropriately. It is Apsiz's responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on / sold to a third party.

6. Data Access & Accuracy

All Individuals / Service Users have the right to access the information Apsiz holds about them. Apsiz will also take reasonable steps to ensure that this information is kept up to date by asking Data Subjects whether there have been any changes i.e. requesting an updated CV from you. In addition, Apsiz will ensure that:

- It has specific responsibility for ensuring compliance with Data Protection
- Everyone processing personal information understands that they are contractually responsible for following good data protection practice
- Everyone processing personal information is appropriately trained to do so

- Everyone processing personal information is appropriately supervised
- Anybody wanting to make enquiries about handling personal information knows what to do
- It deals promptly and courteously with any enquiries about handling personal information
- It describes clearly how it handles personal information
- It will regularly review and audit the ways it holds, manages and uses personal information
- It regularly assesses and evaluates its methods and performance in relation to handling personal information
- All staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 1998 and also the requirements of the General Data Protection Regulation (GDPR) 2018.

Any queries or questions in relation to this policy please contact the Apsiz Services by contacting us on **0800 917 7884** or dropping us an email with an update on your preferences to enquiries@apsiz.co.uk.

Glossary of Terms

- ✓ **Data Controller** – “A person or organisation who determines the purposes for which and the manner in which any personal data are, or are to be, processed” i.e. Apsiz
- ✓ **Data Subject** – “An individual who is the subject of personal data” i.e. Candidates, Clients and / or Leads.
- ✓ **Data Processor** – “Any person (other than an employee of the data controller) who processes the data on behalf of the data controller” i.e. our Applicant Tracking System
- ✓ **Data Protection Act 1998** – The UK legislation that provides a framework for responsible behaviour by those using personal information.
- ✓ **Individual / Service User** – The person whose personal information is being held or processed by Apsiz for example: a client, an employee, or supporter.
- ✓ **Explicit Consent** – is a freely given, specific and informed agreement by an Individual/Service User in the processing of personal information about her/him. Explicit consent is needed for processing sensitive data.
- ✓ **Notification** – Notifying the Information Commissioner about the data processing activities of Apsiz, as certain activities may be exempt from notification. The link below will take to the ICO website where a self-assessment guide will help you to decide if you are exempt from notification: http://www.ico.gov.uk/for_organisations/data_protection/the_guide/exemptions.aspx
- ✓ **Information Commissioner** – The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 1998.
- ✓ **Information Commissioner's Office (ICO)** – the ICO provides independent advice and guidance about data protection and freedom of information. Regular updates can be found on their website: www.ico.gov.uk
- ✓ **Processing** – means collecting, amending, handling, storing or disclosing personal information.
- ✓ **Personal Information** – Information about living individuals that enables them to be identified – e.g. name and address. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers or employees within (GROUP).
- ✓ **Sensitive Data** – refers to data about:
 - Racial or Ethnic Origin
 - Political Affiliations
 - Religion or Similar Beliefs
 - Trade Union Membership
 - Physical or Mental Health
 - Sexuality
 - Criminal Record or Proceedings