C.P. Christodoulou Audit Ltd

Privacy Policy

Data Protection Policy

1. Policy Statement

C.P. Christodoulou Audit Ltd (referred to as "**CPC**" or "**we**" or "**us** "or "**our**") is a company registered in the Republic of Cyprus, under registration number HE393773 as a limited liability company having its registered office at 6, Evagora Papachristoforou Street, 2nd floor, 3030, Limassol, Cyprus.

CPC is committed to protecting and respecting your privacy and handling your personal data in an open and transparent manner. Every day our business will require us to collect and process personal information about our clients. It is important that this information is handled lawfully and appropriately in line with the requirements of the General Data Protection Regulation ("**GDPR**") and any national law supplementing or implementing the GDPR (collectively referred to as the "**Data Protection Requirements**").

2. About This Policy

This policy, and any other documents referred to in it, sets out the basis on which we will process any personal data we collect or process.

This policy does not form part of any contract and may be amended at any time.

CPC is responsible for ensuring compliance with the Data Protection Requirements and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been adhered to should be referred in the first instance to the Data Protection Officer at office@cpcaccountants.com.

For the purposes of this privacy policy:

Personal data means data (whether stored electronically or paper based) relating to a living individual who can be identified directly or indirectly from that data (or from that data and other information in our possession).

Processing is any activity that involves use of personal data. It includes obtaining, recording, or holding the data, organising, amending, retrieving, using, disclosing, erasing, or destroying it. Processing also includes transferring personal data to third parties.

Sensitive personal data includes personal data revealing a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic, biometric, physical, or mental health condition, sexual orientation, or sexual life. It can also include data about criminal offences or convictions. Sensitive personal data can only be processed under strict conditions, including with the consent of the individual.

3. Data Protection Principles

We adhere to the principles relating to processing of personal data set out in the GDPR which require that personal data are:

a. Processed fairly, lawfully and in a transparent manner.

b. Collected for specified, explicit and legitimate purposes and any further processing is completed for a compatible purpose.

c. Adequate, relevant, and limited to what is necessary for the intended purposes.

d. Accurate, and where necessary, kept up to date.

e. Kept in a form which permits identification for no longer than necessary for the intended purposes.

f. Processed in line with the individual's rights and in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

4. What personal data we collect

We may collect your personal data because you give them to us, because other people give that data to us or because it is publicly available. We may also collect personal data from you because we observe or infer that data about you from the way you interact with us.

We may collect the following personal data from you depending on the service we provide to you:

- Contact details such as your name, address, telephone number, e-mail address and fax number.
- Identification details such as your identification or passport number.
- Biographical and demographic data such as your date of birth, age, gender, and marital status.
- Education and employment information including your academic and professional background, employment history, current occupation, and business activities.
- Financial and tax-related information such as your bank account number and account details, your source of income and wealth and your tax residency.
- Details of any complaints or queries you have and for which you have contacted us.
- Details in relation to any transactions you carry out, including the purpose of the transaction, its destination and payee and source details.
- Details in relation to any business activities you carry out.

- Details in relation to any public positions you, or a close relative or close associate of yours, hold or have held in the past.

We may collect the following sensitive personal data depending on the service we provide to you, but only to the extent that we are authorised by law to do so or where we you have given us your explicit consent:

- details in relation to your nationality, and
- details in relation to criminal convictions and offences.

5. Why we need your personal data

a. Personal data

We will only process personal data when the law allows us to. Most commonly, we will use your personal data in the following circumstances:

(a) Where we need to perform the contract, we have entered with you or in order to take certain steps prior to entering a contract with you

Processing is necessary for us in order to provide you with services, and more specifically in order to:

- evaluate the risks, administer, provide and service your contract/business relationship with us.
- communicate with you, in order to service your contract/business relationship with us.
- communicate with you and resolve any complaints and/or enquiries you may have.
- notify you about any changes to our products and/or services; and
- recover any payment due to us in respect of the products and/or services we have provided to you.

The purpose of processing personal data depends on the requirements for each service and the engagement letter provides more details of the relevant purposes.

If you do not provide the personal data, we request from you, we may not be able to offer you our services.

(b) Where we need to comply with a legal obligation

We are required to comply with certain legal and regulatory obligations as well as statutory requirements which may involve the processing of personal data. Such obligations and requirements impose on us necessary personal data processing activities for identity verification, compliance with court orders, tax law or other reporting obligations and anti-money laundering controls.

(c) Where we have appropriate legitimate interests to use your personal data

In some cases, we may process your personal data to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights are not overridden by our interests. More specifically, we may process your personal data in order to:

- maintain our accounts and records.
- enhance the security of our network and information systems.
- identify, prevent, and investigate fraud and other unlawful activities, unauthorised transactions, and other liabilities, and manage risk exposure and quality.
- safeguard the security of our people, premises and assets and prevent trespassing through video surveillance.
- manage our infrastructure, business operations and comply with internal policies and procedures.
- modify, personalise, or otherwise improve our services/communications.
- defend, investigate, or prosecute legal claims; and
- receive professional advice (e.g. tax or legal advice).

(d) Where you have given us your consent

We will only ask for your consent when we wish to provide marketing information to you in relation to our products or services which we believe may be of interest and benefit to.

You may withdraw your consent to such processing at any time. Please note that any processing that was carried out prior to the withdrawal of your consent shall not be affected in any way.

b. Sensitive data

We will only use your sensitive data in the following circumstances:

a. where you have given us your explicit consent to do so, or

b. where processing of your sensitive data is necessary for the establishment, exercise or defence of legal claims which may relate to the service(s) that we provide to you; or

c. where we need to use your sensitive data for reasons of substantial public interest, provided that we are allowed by law to do so, such as obtaining details of your ethnicity in order to carry out anti-money laundering checks.

6. Who we share your personal data with

During the performance of our contractual and statutory obligations, your personal data may be disclosed to various service providers, partners, and suppliers. Such third parties enter contractual

arrangements with CPC by which they are required to comply with confidentiality and data protection obligations according to the Data Protection Requirements.

We may disclose data about you for any of the reasons set out above, or if we are legally required to do so, or if we are required under our contractual or statutory obligations.

Under the circumstances referred to above, recipients of personal data may be for example:

- any member in our group of companies.
- service providers we have chosen to support us in the effective provision of our services to you by offering technological expertise, solutions, and support.
- auditors and accountants.
- external legal consultants.
- file storage companies, archiving and/or records management companies, and cloud storage companies.
- financial and business advisors.
- governmental and regulatory bodies, including law enforcement authorities, in connection with enquiries, proceedings or investigations by such parties or in order to enable Abacus to comply with its legal and regulatory obligations.
- credit reference agencies or other organisations that help us make business decisions and mitigate the risk of potential fraud and misconduct.
- third parties who may be involved in a potential or actual sale of all or a portion of CPC's business or assets, and/or
- banks and financial institutions.

Some of the recipients of your personal data may be in third countries (i.e. countries outside the European Economic Area). We will ensure that all such recipients comply with applicable Data Protection Requirements and have in place appropriate safeguards in relation to the transfer and use of your data.

7. How long we keep your personal data for

We will keep your personal data for as long as we have a business relationship with you. Once our business relationship with you has ended, we may keep your personal data for the longest of the following periods: (i) any retention period set out in our retention policy which is in line with regulatory requirements relating to retention; or (ii) the end of the period in which legal action or investigations might arise in respect of the services provided. We may keep your data for longer if we cannot delete it for legal, regulatory, or technical reasons. If we do, we will make sure that your privacy is protected and that your data are only used for those purposes.

8. Your data protection rights

Under the GDPR you have a number of rights with regard to your personal data. In particular, you have the right to:

- **Request access** to your personal data. This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal data that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have exercised your right to object to processing.
- **Object to processing** of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to the processing on this ground.

  Request the restriction of processing of your personal data. This enables you to ask us to suspend the processing of personal data about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of your data to another party.

In the limited circumstances where you may have provided your consent for the processing of your data you have the right to withdraw that consent at any time which will not affect the lawfulness of the processing before your consent was withdrawn. To withdraw your consent, please contact office@cpcaccountants.com. Once we have received notification that you have withdrawn your consent, we will no longer process your data for the purpose you originally agreed to, unless we have another legitimate basis for doing so.

You have the right to lodge a complaint to the Office of the Commissioner for Personal Data Protection if you have any complaints in relation to the manner Abacus has handled any request you have made in relation to your personal data or to how it otherwise handles your personal data.

9. Data Security

We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental or unlawful destruction, damage, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored, or otherwise processed.

We will put in place procedures and technologies to maintain the security of all personal data from the point of the determination of the means for processing and point of data collection to the point of destruction. Personal data will only be transferred to a data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

We will maintain data security by protecting the confidentiality, integrity, and availability of the personal data, defined as follows:

a. **Confidentiality** means that only people who are authorised to use the data can access it.
b. **Integrity** means that personal data should be accurate and suitable for the purpose for which they are processed.
c. **Availability** means that authorised users should be able to access the data if they need it for authorised purposes.

Security procedures include:

a. **Entry controls.**

b. **Secure lockable desks and cupboards.** Desks and cupboards are kept locked if they hold confidential information of any kind. Abacus follows a clean desk policy.

c. **Pseudonymisation and encryption of data.**

d. **Methods of disposal.** Paper documents are shredded. Digital storage devices are physically destroyed when they are no longer required.

e. **Equipment.** Staff always ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

f. **Secure archive infrastructure.** All record keeping areas are protected by appropriate fire detection, automatic firefighting systems, pest control systems and anti-theft systems. Access to such areas is restricted and controlled.

10. Changes to this Policy

We may modify or amend this privacy policy from time to time.

We will notify you appropriately when we make changes to this privacy policy and we will amend the revision date at the bottom of this page. We do however encourage you to review this policy periodically so as to be always informed about how we are processing and protecting your personal information.

11. Data Protection Officer

If you have any concerns or questions as to how your personal data is processed or if you wish to exercise any of your rights (set out in paragraph 8 above) you can contact:

Costas Christodoulou, Data Protection Officer at: costas@cpcaccountants.com.