

# Zavros Mintikkis Associates Limited – Privacy Policy

## Introduction

In the course of its business, the Firm needs to gather and use certain information about individuals. This will include clients, suppliers and other business contacts, and employees and prospective employees, as well as other people that we have a relationship with, may need to contact, or with whom we need to deal.

This policy describes how this personal data must be collected, processed, transferred, handled and stored in order to meet the requirements of data protection law, in particular the General Data Protection Regulation (GDPR). We recognise that, not only must we comply with the principles of fair processing of personal data, we must also be able to demonstrate that we have done so. The procedures and principles set out below must be followed at all times by the Firm, its employees and all those within its scope as set out below.

## Why this policy exists

This Policy provides help and guidance to our staff and managers in:

- complying with data protection law and following good practice
- protecting the rights of staff, clients, partners and business contacts
- being open about how we use personal data, how we store it and when we secure it
- protecting the Firm against the risks of both inadvertent and intentional data breaches

## Scope of the Policy

The Policy applies to all employees; fixed term contract employees; temporary employees; agency staff; and consultants and contractors who are provided with access to any of the Firm's files and/or computer systems. Collectively these individuals are hereafter referred to as 'users'. All users have responsibility for complying with the terms of this Policy.

## Data Protection Law

### What is personal data?

The GDPR regulates how organisations must collect, handle and store personal data. Personal data is any information relating to an identified or identifiable living individual. It is information which enables that person to be identified, directly or indirectly, and may include their name, address, telephone number(s), email address(es), age, location data, or online and biometric identifiers. We hold data relating to our employees, some of which is classed as sensitive personal data (also known as 'special category data') where, for example, it concerns a person's health and medical status. We also hold a wide range of information about clients, including highly confidential personal financial data such as their individual tax information.

These rules apply to all data stored in any structured way, including both paper files and electronically.



## What does the law say?

### The Data Protection Principles

The GDPR contains a number of key principles which apply to the collection and processing of personal data and which underpin everything that follows.

Lawfulness, fairness and transparency	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject
Purpose limitation	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
Data minimisation	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
Accuracy	Personal data shall be accurate and, where necessary, kept up to date
Storage limitation	Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
Integrity and confidentiality	Personal data shall be processed 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
Accountability	The controller shall be responsible for, and be able to demonstrate compliance with the GDPR

For the purposes of the law and these principles, a 'data controller' is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed. In relation to the majority of our data, we are data controllers, although where we are responsible for e.g. looking after a client's payroll, they are the data controller and we are 'data processors'. A data processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller." Our responsibilities as data processors are dealt with later in the Policy.

## Key Responsibilities

- The Directors are ultimately collectively responsible for ensuring that the Firm meets its legal obligations and that this Policy is followed
- John Mintikkis, the Data Protection Officer (DPO) is responsible for:
  - keeping the directors updated about data protection responsibilities, risks and issues
  - reviewing all data protection procedures and related policies, in line with an agreed schedule
  - arranging data protection training and advice for everyone to whom this Policy applies
  - handling data protection queries from staff and contractors
  - dealing with requests from anyone whose data we hold for access to that data (known as 'subject access requests')
  - checking and approving any contracts or agreements with third parties that may handle our personal data
  - checking and approving any contracts or agreements with third parties whose personal data we may handle
  - ensuring that policies on processing, retention, storage and deletion of data are adhered to and relevant documentation is maintained to evidence compliance
- The IT Manager, John Mintikkis is responsible for:
  - ensuring that all systems, services and equipment used for storing data meet acceptable security standards
  - performing regular checks to ensure that security hardware and software is functioning properly
  - evaluating any third-party services the Firm is considering using to store or process data. For example, cloud computing services
- John Mintikkis & Nick Zavros, the directors in charge of Marketing, are responsible for:
  - approving any data protection statements attached to communications such as emails and letters
  - where necessary working with other staff to ensure marketing initiatives are compliant with data protection principles
  - ensuring that records of consents and withdrawal of consents to marketing are maintained.

## Lawful, Fair and Transparent Data Processing

We are responsible as a Firm for ensuring that any personal data we hold is processed in accordance with the principles laid out above. We are permitted to process data where one of the following legal bases applies:

- the data subject has given their **consent**. An example might be where a client has agreed to be contacted about a new tax advice service we are providing
- the processing is necessary for the **performance of a contract** to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering a contract with them. An example of this is where we need to retain and file personal information about our clients in order to finalise their accounts or tax affairs, or where a potential client gives us their personal data in order for us to be able to quote for advice that they need, and in order for them to decide whether to instruct us
- the processing is necessary for **compliance with a legal obligation** to which the data controller is subject. An example of this might be where we pass personal data to the relevant money laundering authorities in a situation where we have an obligation to do so
- the processing is necessary to **protect the vital interests of the data subject** or another natural person. An example of this might be where we pass on information to the next of kin of an employee who is gravely ill
- the processing is necessary for the **performance of a task carried out in the public interest** or in the exercise of official authority vested in the data controller. This is usually used by public authorities carrying out vital functions such as provision of public utilities or public safety
- the processing is necessary for the purposes of **legitimate interests** pursued by the data controller or by a third party, except where those interests are overridden by the fundamental rights and freedoms of the data subject and their right to privacy in relation to their personal data. This is a difficult exception to generalise about, but it can be used by business where they have legitimate commercial aims which can override the data subjects' interests. An example might be the chasing of a legitimate debt, investigating potential dishonesty of an employee, investigating a grievance about sexual or racial harassment. These legitimate aims may require some processing of personal data which may be justified in that context. Any user who wishes to use this basis would be advised to speak to the DPO to discuss it.

## Sensitive Personal Data or 'Special Category Data'

This data has a special status under the law, as it is particularly personal in nature. It concerns a person's race, ethnicity, politics, religion, trade union membership, genetics, biometrics used for identification purposes, health, sex life or sexual orientation. There are a number of strict rules about the processing of this kind of data, and the kinds of situations in which it is legitimate to process it, and usually the data controller needs the data subject's explicit consent to do so or a clear legal basis. We will never disclose such data to any third party unless legally obliged to do so, and then only to appropriate authorities as required by law.



## Other Personal Data

The Firm will adhere to the following principles:

- the Firm collects and processes the personal data set out in **XX** below, this includes:
  - personal data obtained directly from data subjects, and
  - personal data obtained from third parties
- the Firm only collects processes and holds personal data for the specific purposes set out in **xx** below, or for other purposes expressly permitted by the GDPR
- we keep data subjects informed at all times of the purpose(s) for which the Firm processes their personal data
- where personal data will be disclosed to third parties, we will only do so where we are legally required to do so, e.g. to HMRC or to money laundering authorities, or where we have the data subjects' free and informed consent to the disclosure
- we will only collect and process personal data for and to the extent necessary for those specified purpose(s)
- in respect of personal data that we collect and process, we will
  - keep it accurate and up to date
  - grant the data subject the right to rectify any inaccurate data in accordance with their right to do so
  - regularly check the data and ensure that all reasonable steps are taken to promptly rectify or delete any mistakes or inaccuracies as appropriate
  - not keep personal data any longer than is necessary bearing in mind the purpose(s) for which it was collected
  - take all reasonable steps to delete or dispose any data which is no longer required promptly
  - adhere to our Retention Policy, which is available to all staff
  - take measures to ensure the security of the data in line with the measures set out below

## Data Processing

We act as data processors for a number of clients (the data controllers), receiving personal data relating to their employees and processing it for payment of salary, and appropriate deductions. We do not expect to receive any data which is sensitive personal data in relation to this. We will:

- only process the personal data provided in accordance with the data controller's instructions and in accordance with our contract with them
- implement technical and organisational measures in line with the GDPR to ensure the fair and lawful processing and the security of such data
- not disclose the data or transfer it to any third party without the explicit permission of the data controller, unless we are legally obliged to do or it is permitted and authorised by the contract with the data controller
- ensure that appropriate records are kept in order that we are able to demonstrate compliance with GDPR principles
- comply with our obligations to notify the regulatory authorities of any data breach.

## Accountability and Record Keeping

The Firm will keep written internal records of all personal data collection, holding and processing, and this will incorporate the following:

- name and details of the Firm, its DPO and any third-party data processors
- the purposes for which the Firm collects, holds and processes personal data
- details of the categories of personal data collected, held and processed by the firm and the categories of data subject to which the data relates
- details of any transfers of data to non-EEA countries including the mechanism for doing so and security measures taken
- details of the Firm's retention policy (see Data Retention Policy)
- detailed descriptions of all technical and organisational measures taken by the Firm to ensure the security of personal data.

### **Privacy by Design – Data Impact Assessments**

Part of the Firm's duty is to ensure that in the planning of new processes or procedures which involve the use of personal data, we consider the impact of the changes and ensure that we have fully considered and complied with our obligations under the GDPR. The Firm will always ensure that all such changes are designed and implemented in accordance with the Regulation, and that the DPO is consulted and their recommendations are taken into account in the planning and introduction of such changes.

In any situation where new technologies are being deployed and the processing of the personal data is likely to result in a high risk to the data subjects' rights and freedoms under the Regulation, we will carry out a Data Impact Assessment, overseen by the DPO. This will deal with:

- the type(s) of personal data that will be collected, held and processed
- the purpose for which it is to be used
- the Firm's objectives in processing this data and making this innovation
- how the personal data is to be used
- internal and external parties to be consulted
- why we need the data and how the collection of the data is proportionate to our need for it
- what risks there are for data subjects
- what risks the Firm runs, and
- what measures we are proposing to minimise and protect against the risks.

### **Providing Information to Data Subjects**

We are required to ensure that, when we collect and process personal data, the data subject is aware of the purposes for which this is being done, and what is happening to the data. We therefore will ensure that the following principles are followed:

- where we collect personal data directly from the data subject, we will inform them of the purpose for which it is being collected at the time of collection
- where we are obtaining personal data from a third party, we will inform the data subject why we are doing this
  - if we use the details to contact them, at the time of first contact, or
  - if we are going to pass the information to a third party, at the time this is done, or
  - as soon as is reasonably possible and in any event, within one month

- All data subjects will be provided with the following information:
  - details of the Firm, including the name of the DPO
  - why the data is being collected and processed, and the legal basis for this
  - if applicable, any legitimate interests justifying the Firm's collection and processing of data
  - where personal data is not collected directly from the subject, the categories of data collected and processed
  - where the data is to be transferred to third party/parties, their details
  - where data is to be transferred outside EEA, details of the transfer
  - details of data retention
  - details of the data subject's rights
    - under GDPR
    - to withdraw consent to processing at any time
    - to complain to the Information Commissioner's Office (ICO)
  - details of any legal or contractual requirement which means that the Firm needs to collect this information and process it, and what the implications are if it cannot do so.
  - details of any automated decision making or profiling that will take place using personal data, how the decisions will be made and their consequences

### **Data Subject Access**

'Subject Access Requests' (SARs), can be made by data subjects where an organisation holds personal data about them. This can be done at any time, and the requests are made in order for the data subject to find out what data is being held, and what is being done with it.

*Where a subject access request is being made to us as a payroll processor, we will refer the employee to the data controller (who is their employer or client) to deal with the request.*

- such requests need to be made by the data subject in writing
- they should be addressed to the DPO, who will deal with the request
- the Firm will usually respond to them within one month, but we may need to extend it for a period of up to a further two months if it is a complex request or there are multiple requests. In that situation, the data subject(s) will be informed.
- the Firm will not charge the data subject any fee for responding to the SAR, unless the subject is asking for multiple copies of data already supplied or unless the request is manifestly unfounded or excessive.

### **Rectification of Personal Data**

Where a data subject informs us that data we are holding about them is inaccurate or incomplete and requests that it is corrected, we will rectify the information and inform the data subject that we have done so, within one month of the request. Again, in complex cases, we may extend that period by up to two months.

Where the incorrect data is held by third parties to whom it has been disclosed, we will ensure that they are informed and that the data that they hold is rectified.



## **Erasure of Personal Data**

Data subjects have a right to require the Firm to erase personal data held about them when:

- the Firm no longer needs the data it is holding for the purposes for which it was originally collected
- the data subject wishes to withdraw their consent to the Firm holding and processing the data
- the data subject objects to the Firm holding and processing the data, and there is no overriding legitimate interest which allows us to continue to do so
- the personal data has been processed unlawfully
- the personal data needs to be erased in order for the Firm to comply with a particular legal obligation.

Where we are obliged to do so, we will erase the information and inform the data subject that we have done so, within one month of the request. Again, in complex cases, we may extend that period by up to two months, and again where the data is held by third parties to whom it has been disclosed, we will ensure that they are informed and that the data that they hold is erased.

## **Restriction of Personal Data Processing**

Data Subjects have a right to request that the Firm ceases to process any personal data that we are holding about them. If that takes place, we will only retain whatever personal data we need to ensure that no further processing takes place, and we will inform any third parties to whom we have disclosed the data about the restriction on processing (unless it is impossible to do so or would involve disproportionate effort).

## **Objections to Personal Data Processing**

Data subjects have a right to object to us processing their personal data based on our legitimate interests or for direct marketing purposes. Where the data subject notifies us of their objection, we will cease such processing immediately unless our legitimate interests override those of the data subject, or unless we need to continue to process the data in conducting a legal claim. Where the data subject is objecting to direct marketing, we will cease to use the data for this purpose immediately.





## Personal Data, Collected, Held and Processed

Type of Data	Purpose
Personal details of employees, such as names, addresses, contact details, age, sex etc	The administration of Payroll services for clients
Personal details of clients, such as names addresses, contact details, age, sex etc	To provide accountancy and related services to clients, in particular for the administration of their tax and personal financial affairs and to comply with both their and our legal obligations including in relation to tax and money laundering.  To market our services to clients, in accordance with the GDPR
Education and Training details of our prospective employees, employees and contractors	Collected in the course of recruitment with a view to selection, and maintained to track their career progression
Financial Details of employees and contractors i.e. matters related to income and payroll, tax details, expenses claimed, court orders, pensions, insurance	Collected and maintained in order to ensure timely and accurate payment of staff, and proper accounting for tax purposes

## Data Security – Transferring Personal Data and Communications

We will ensure that we take the following measures with respect to all communications containing personal data:

- all emails containing personal data are encrypted using Microsoft [insert the system used here)
- all documents prepared for clients such as tax returns, and final accounts will be held in a separate on the main server in ZMA's offices. Access to the area is controlled and only accessible by ZMA staff.
- all emails containing personal data will be marked 'Confidential'
- Personal data will be sent as an attachment to the e mail and be password protected. This is especially the case when sending Tax Returns and Payroll information, such as payslips
- personal data contained in the body of an email, whether sent or received, should be copied from the body
- all temporary files containing any personal data should be deleted without delay
- all personal data sent in hard copy form should be delivered to the recipient in person, in a container marked 'Confidential', or sent by recorded delivery or courier, as appropriate.

## **Data Storage and General Security**

For detailed guidance on this please refer to NCSC Cyber Essentials at [www.cyberessentials.ncsc.gov.uk](http://www.cyberessentials.ncsc.gov.uk).

- all electronic copies of personal data should be stored securely using privilege levels and passwords
- regular password changes will be enforced, and the number of logins will be restricted
- passwords should never be written down or shared between any employees, agents, contractors or other persons working on behalf of the Firm, no matter what their level of seniority.
- computer equipment belonging to the Firm will be sited in a secure location within the office and in a position where they cannot be viewed by members of the public
- computer terminals must not be left unattended, and should be logged off at the end of the session
- personal data is backed up daily and is store offsite location and where appropriate is encrypted
- all software must be kept up to date and John Mintikkis shall be responsible for ensuring that all security-related updates are installed promptly, unless there are valid technical reasons for not doing so
- no software should be installed on the Firm's system without the prior approval of John Mintikkis
- personal data should not be stored on any mobile device such as laptops, tablets and smartphones without the approval of the DPO and, where it is held, only in accordance with his or her instructions and limitations.
- personal data must never be transferred on to an employee's personal device and we will never transfer such data onto a device owned by a contractor or agent unless they have agreed to comply fully with the letter and spirit of this Policy and with the GDPR
- all manual files must be stored securely in locked cabinets and should not be left unsecured in the office overnight
- computer print outs containing personal information should be destroyed without delay and should never be retained for scrap paper
- where personal data is to be erased, or otherwise disposed of, this will be done in accordance with the Firm's Data Retention Policy.

## **Access to Personal Data**

In relation to accessing personal data:

- employees must never access data either on a computer or in paper form, without having authority to do so
- personal data must not be shared informally and if an employee, agent, contractor, or any other third party wants access to the data, it must be formally requested from the DPO
- personal data must be handled with care, and should not be left unattended or in view of unauthorised employees, contractors or agents whether on paper or on a screen
- where personal data held by the Firm is being used for marketing purposes, it is the responsibility of John Mintikkis to ensure that appropriate consents are obtained.

## **Organisational Measures**

The Firm will take the following steps in relation to the collection, holding and processing of personal data:

- all employees, agents, contactors or other parties working on our behalf will be made fully aware of their individual responsibilities, and the responsibilities of the Firm, in relation to data privacy and the GDPR and they will be provided with a copy of this Policy
- in respect of these individuals and of personal data held by the Firm:
  - only those persons who need access to particular personal data in order to complete their assigned duties will be granted such access
  - all persons will be appropriately trained and supervised in handling personal data
  - all persons will be encouraged to exercise caution in discussing work related matters within the workplace
  - all employees are bound by strict duties of professional confidentiality in discussing any work-related matters outside the workplace, which will be adhered to and enforced
- our methods of collecting, holding and processing data will be regularly evaluated and reviewed and the personal data held by the Firm will be reviewed periodically, as set out in our Data Retention Policy
- we will keep the performance of our agents, contractors and third parties under review and, not only will we ensure that they are required to handle personal data in accordance with the GDPR and our Policy, but we will also ensure that they are held to the same standards as our own employees both contractually and in practice
- where any agent, contractor or third party fails in their obligations under this Policy, we will ensure that they are required to indemnify us for costs, losses, damages or claims which may arise as a result.

## **Transfer of Personal Data outside the EEA**

The Firm may from time to time transfer personal data outside the EEA. This will only be done if one or more of the following applies to the transfer:

- it is to a territory or sector within that territory that the European Commission has determined has an adequate level of protection for personal data, or appropriate safeguards as determined by the supervisory authorities
- it is made with the informed consent of the data subject
- it is necessary for the performance of a contract between the data subject and the Firm, or for pre-contractual steps taken at the request of the data subject
- it is necessary for important public interest reasons, or for the conduct of legal claims, or to protect the vital interests of the data subject
- it is made from a register that under UK or EU law is intended to provide information to the public and which is open to the public or to those able to show a legitimate interest in accessing it.

### **Data Breach Notification**

All personal data breaches must be reported immediately to the DPO.

If such a breach occurs, and it is likely to result in a risk to the rights and freedoms of data subjects e.g. financial loss, breach of confidentiality, reputational damage, the DPO is required to ensure that the ICO is informed without delay and, in any event, within 72 hours of the breach.

Where the breach is likely to result in a high risk to the rights and freedoms of data subjects, the DPO also needs to ensure that the data subjects affected by the breach are informed directly and without undue delay. The following information must be provided:

- the categories and approximate numbers of data subjects affected
- the categories and approximate numbers of personal data records concerned
- the name and contact details of the Firm's DPO
- the likely consequences of the breach
- details of the measures taken, or proposed, to deal with the consequences of the breach.

