



## **PRIVACY NOTICE issued by Acc-Unique Solutions Ltd**

### **Introduction**

The Data Protection Act 2018 (“DPA 2018”) and the General Data Protection Regulation (“GDPR”) impose certain legal obligations in connection with the processing of personal data.

Acc-Unique Solutions Ltd is a data controller within the meaning of the GDPR and we process personal data. The firm’s contact details are as follows: Fiona Wilson (the Data Protection Officer), Acc-Unique Solutions Ltd, Grosvenor House, 11 St Paul’s Square, Birmingham, B3 1RB.

We may amend this privacy notice from time to time. If we do so, we will supply you with and/or otherwise make available to you a copy of the amended privacy notice.

Where we act as a data processor on behalf of a data controller (for example, when processing payroll), we provide an additional schedule setting out required information as part of that agreement. That additional schedule should be read in conjunction with this privacy notice.

### **The purposes for which we intend to process personal data**

We intend to process personal data for the following purposes:

- To enable us to supply professional services to you as our client.
- To fulfil our obligations under relevant laws in force from time to time (e.g. the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (“MLR 2017”).
- To comply with professional obligations to which we are subject as a member of AAT (The Association of Accounting Technicians)
- To use in the investigation and/or defence of potential complaints, disciplinary proceedings and legal proceedings.
- To enable us to invoice you for our services and investigate/address any attendant fee disputes that may have arisen.
- To contact you about other services we provide which may be of interest to you if you have consented to us doing so.

### **The legal bases for our intended processing of personal data**

Our intended processing of personal data has the following legal bases:

- The processing is necessary for the performance of our contract with you.
- The processing is necessary for compliance with legal obligations to which we are subject (e.g. MLR 2017).

It is a requirement of our contract with you that you provide us with the personal data that we request. If you do not provide the information that we request, we may not be able to provide professional services to you. If this is the case, we will not be able to commence acting or will need to cease to act.

### **Data may be collected from:**

Clients, Clients’ customers, suppliers, banks, government agencies, debt collectors



**The type of Information we collect, the reason for collecting it and the source of the information:**

Client Data - personal details of business owners and directors, including copy documentation for identification, completed client registration forms, copy letters of engagement, bank details, legislative information, contact information, including email addresses, telephone numbers and postal addresses and records of communications and interactions.

We hold the data so that we can carry out identity checks on clients for money laundering requirements, provide bank signatory services for clients as required and to document the services that we provide to clients and inform them of our terms.

We obtain the data from new clients at initial appointment

Payroll and CIS Services - dates of birth, marital status, income, individual's personal information such as starter and leaver dates, changes of address and status as well as cyclical information such as timesheet information, pay rise notifications, bonuses and pay elements, sick notes

We hold the data to enable us to process payroll procedures, submit figures to government agencies and calculate figures for accounts and bookkeeping procedures

We obtain the data from the client, doctors and government agencies

Bookkeeping and Vat Services – supplier correspondence, customer correspondence, bookkeeping documents, bank details, price lists, working papers, vat documentation and transactions

We hold the data to enable us to process bookkeeping procedures, submit returns to government agencies, provide company performance reports and to prepare year end accounts.

We obtain the data from the client, suppliers, customers and HMRC

Tax Services - Authentication codes for Companies House, Registered Office Details, tax correspondence

We hold the data to enable us to process and submit statutory returns to government agencies

We obtain the data from Clients, government agencies

Training Services – Delegate booking forms, contact information and payment details.

Sensitive information such as initial assessment questionnaires, additional learning requirements, log of prior experience, qualifications, completed assessment activities

We hold the data to enable us to book clients onto our courses, assess training requirements, monitor improvement and process payments

We obtain the data from Delegates and their colleagues

Secretarial Services – Course and club member contact details (work and personal), qualifications and employment grades, records of communications and interactions, employer name and address, personal and work telephone numbers, dietary requirements

We hold the data to enable us to book delegates onto client's training courses, provide course information, certificates of attendance and manage sponsorship



## Persons/organisations to whom we may give personal data

We may share your personal data with:

- HMRC
- any third parties with whom you require or permit us to correspond
- subcontractors
- an alternate appointed by us in the event of incapacity or death
- tax insurance providers
- professional indemnity insurers
- our professional body, AAT (Association of Accounting Technicians and the Office of Professional Body Anti-Money Laundering Supervisors (OPBAS) in relation to practice assurance and the requirements of MLR 2017 (or any similar legislation)

If the law allows or requires us to do so, we may share your personal data with:

- the police and law enforcement agencies
- courts and tribunals
- the Information Commissioner's Office ("ICO")

We may need to share your personal data with the third parties identified above in order to comply with our legal obligations, including our legal obligations to you. If you ask us not to share your personal data with such third parties, we may need to cease to act.

## Security of Data

We undertake an analysis of the risks presented by our processing and use this to assess the appropriate level of security we need to put in place. We have an information security policy (or equivalent) and take steps to make sure the policy is implemented. We make sure that we regularly review our information security policies and measures and, where necessary, improve them. We have put in place basic technical controls such as those specified by established frameworks like Cyber Essentials. We use encryption where it is appropriate to do so. We make sure that we can restore access to personal data in the event of any incidents, such as by establishing an appropriate backup process.

## Personal Data Breach

If your personal data has been breached, we will inform you directly if we believe your rights and freedoms have been significantly put at risk as a result. We will clearly describe the nature of the breach, its likely consequences and the measures we have taken to prevent further occurrences.

An assessment will be made as to whether there is a likely risk to any person's rights and freedoms as a result of the breach. This would result in a requirement to report to the ICO.

All personal data breaches will be recorded and documented by us, regardless of the decision to report the breach to the ICO. Our documentation will include the details of the breach and any remedial action we plan to take to prevent further breaches occurring.

## Transfers of personal data outside the EEA

Data is encrypted using AES 256-bit encryption and stored in Microsoft Office 365 applications, using file-level **encryption** to **encrypt data** at rest. Office 365 moves beyond a single **encryption** key per disk to deliver a unique **encryption** key so that every file stored in SharePoint Online, including **OneDrive** folders is **encrypted** with its own key.

## Retention of personal data

When acting as a data controller and in accordance with recognised good practice within the tax and accountancy sector we will retain all records relating to you as follows:

- Where we have an ongoing client relationship involving data which is needed for one or more year's tax compliance (e.g. tax returns, capital gains base costs and claims and elections submitted to HMRC), the data will be retained for 6 years plus the current year.
- where ad hoc training/advisory work has been undertaken it is our policy to retain information for 2 years from the date the business relationship ceased.
- Where the business relationship has ended data will be deleted after 7 years unless you as our client ask us to retain it for a longer period.

All documents are kept on a secure cloud-based portal that you as a client will have access to at all times. This service is provided free of charge to clients. The details of this cloud service provider are: Docsafe, 3 Brindley Place, Birmingham, B1 2JB. Telephone: 0121 794 0685. [www.doc-safe.co.uk](http://www.doc-safe.co.uk). VAT Registration No. GB 748228902.

Our contractual terms provide for the destruction of documents after 7 years and therefore agreement to the contractual terms is taken as agreement to the retention of records for this period, and to their destruction thereafter.

You are responsible for retaining information that we send to you (including details of capital gains base costs and claims and elections submitted) and this will be supplied in the form agreed between us. Documents and records relevant to your tax affairs are required by law to be retained by you as follows:

### *Individuals, trustees and partnerships*

- with trading or rental income: five years and 10 months after the end of the tax year;
- otherwise: 22 months after the end of the tax year.

### *Companies, LLPs and other corporate entities*

- six years from the end of the accounting period.

Where we act as a data processor as defined in DPA 2018, we will delete or return all personal data to the data controller as agreed with the controller and at the end of the contract.

## Employees and Interested Parties

The policy applies to all Employees [and interested parties] of **Acc-Unique Solutions Limited** such as outsourced suppliers. Any breach of the GDPR will be dealt with under the firm's disciplinary policy and may be a criminal offence, in which case the matter must be reported as soon as possible to the appropriate authorities.

Partners and any third parties working with or for the firm, and who have or may have access to personal information, are expected to have read, understood and to comply with this policy.

No third party may access personal data held by the firm without having first entered into a data confidentiality agreement, which imposes on the third party obligations no less onerous than those to which the firm is committed, and which gives the firm the right to audit compliance with the agreement.

## **Requesting personal data we hold about you (subject access requests)**

You have a right to request access to your personal data that we hold. Such requests are known as 'subject access requests' ("SARs").

Please provide all SARs in writing marked for the attention of Fiona Wilson.

To help us provide the information you want and deal with your request more quickly, you should include enough details to enable us to verify your identity and locate the relevant information. For example, you should tell us:

1. your date of birth
2. previous or other name(s) you have used
3. your previous addresses in the past five years
4. personal reference number(s) that we may have given you, for example your national insurance number, your tax reference number or your VAT registration number
5. what type of information you want to know

If you do not have a national insurance number, you must send a copy of:

- the back page of your passport or a copy of your driving licence; and
- a recent utility bill.

DPA 2018 requires that we comply with a SAR promptly and in any event within one month of receipt. There are, however, some circumstances in which the law allows us to refuse to provide access to personal data in response to a SAR (e.g. if you have previously made a similar request and there has been little or no change to the data since we complied with the original request).

We will not charge you for dealing with a SAR.

You can ask someone else to request information on your behalf – for example, a friend, relative or solicitor. We must have your authority to respond to a SAR made on your behalf. You can provide such authority by signing a letter which states that you authorise the person concerned to write to us for information about you, and/or receive our reply.

Where you are a data controller and we act for you as a data processor (e.g. by processing payroll), we will assist you with SARs on the same basis as is set out above.

## **Putting things right (the right to rectification)**

You have a right to obtain the rectification of any inaccurate personal data concerning you that we hold. You also have a right to have any incomplete personal data that we hold about you completed. Should you become aware that any personal data that we hold about you is inaccurate and/or incomplete, please inform us immediately so we can correct and/or complete it.

## **Deleting your records (the right to erasure)**

In certain circumstances you have a right to have the personal data that we hold about you erased. Further information is available on the ICO website ([www.ico.org.uk](http://www.ico.org.uk)). If you would like your personal data to be erased, please inform us immediately and we will consider your request. In certain circumstances we have the right to refuse to comply with a request for erasure. If applicable, we will supply you with the reasons for refusing your request.

## **The right to restrict processing and the right to object**



In certain circumstances you have the right to 'block' or suppress the processing of personal data or to object to the processing of that information. Further information is available on the ICO website ([www.ico.org.uk](http://www.ico.org.uk)). Please inform us immediately if you want us to cease to process your information or you object to processing so that we can consider what action, if any, is appropriate.

### **Obtaining and reusing personal data (the right to data portability)**

In certain circumstances you have the right to be provided with the personal data that we hold about you in a machine-readable format, e.g. so that the data can easily be provided to a new professional adviser. Further information is available on the ICO website ([www.ico.org.uk](http://www.ico.org.uk)).

The right to data portability only applies:

- to personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means

We will respond to any data portability requests made to us without undue delay and within one month. We may extend the period by a further two months where the request is complex or a number of requests are received but we will inform you within one month of the receipt of the request and explain why the extension is necessary.

### **Withdrawal of consent**

Where you have consented to our processing of your personal data, you have the right to withdraw that consent at any time. Please inform us immediately if you wish to withdraw your consent.

Please note:

- the withdrawal of consent does not affect the lawfulness of earlier processing
- if you withdraw your consent, we may not be able to continue to provide services to you
- even if you withdraw your consent, it may remain lawful for us to process your data on another legal basis (e.g. because we have a legal obligation to continue to process your data)

### **Automated decision-making**

We do not intend to use automated decision-making in relation to your personal data.

### **Complaints**

If you have requested details of the information we hold about you and you are not happy with our response, if you wish to make a complaint to us about how we use your personal information or you think we have not complied with the GDPR or DPA 2018 in some other way, you can send a complaint directly to us. Complaints should be sent to Fiona Wilson by e-mail using the following e-mail address: [enquiries@acc-uniquesolutions.co.uk](mailto:enquiries@acc-uniquesolutions.co.uk). Alternatively, they can be sent by letter to [Acc-Unique Solutions Ltd, Grosvenor House, 11 St Paul's Square, Birmingham, B3 1RB](#). We will acknowledge receipt of the complaint within 3 working days and will then deal with the issue, informing you of the outcome without undue delay.

If you are not happy with our response, you have a right to lodge a complaint with the ICO ([www.ico.org.uk](http://www.ico.org.uk)).