

Adminrescue Limited

PRIVACY NOTICE

SHORT FORM

We Adminrescue Limited are the data controllers. The firm's Data Protection Officer is Jon Sharpe and can be contacted via email at jonsharpe@adminrescue.co.uk.

We collect the data you give us and which we receive from your employer or colleagues, your customers, your employers other advisers, Credit Reference Agencies, Local Authorities, HMRC, Xama Technologies

We use your personal data to set up and manage our relationship with your employer, to carry out required checks, to meet professional obligations and to comply with the law. This may include informing HMRC, your employer, your spouse/partner, the police and others.

Your data is stored on the systems we use including cloud based systems. On some occasions, we may have to use services outside of the United Kingdom or EU. When this occurs, we will put in place all measures required by law.

We share data with our insurers, external parties we use to provide us with services and various local and national authorities.

We keep your data for the period we have a relationship with your employer plus 7 years unless there are reasons to retain it for longer.

You have the right of access to data, to rectify it, challenge or block its use, to its erasure, move it to another provider and to withdraw consent. You can access these rights by contacting us above.

We do not use automated profiling.

LONG FORM

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.

Adminrescue Limited is a data controller within the meaning of the GDPR and we process personal data. The firm's Data Protection Officer is Jon Sharpe and can be contacted via email at jonsharpe@adminrescue.co.uk.

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 Institute of Certified Bookkeepers (ICB).
- 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:

- Where at the time you gave consent.
- The processing is necessary to carry out pre-contractual steps at your request
- 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).
- The processing is necessary for the purposes of our and others legitimate interests of ours and others including society.

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.

Persons/organisations to whom we may give personal data

We may share your personal data with:

- Your employer, their legal and other advisers and insurers and other parties they engage
- HMRC
- any third parties with whom your employer requires or permits 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 and/or the Office of Professional Body Anti-Money Laundering Supervisors (OPBAS) in relation to practice assurance and/or the requirements of MLR 2017 (or any similar legislation)
- your partners or spouse/partner
- Client Engager (to deliver part of our services to you)
- Our professional indemnity insurers, their lawyers and other advisers

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

- the police and law enforcement and other government 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 and/or your employer and for our and others legitimate interests including of society as a whole. If you ask us not to share your personal data with such third parties we may need to cease to act.

We use certain Cloud based systems to handle your personal data including Client Engager Online, Office 365, Outlook, QuickBooks, Xero, FreeAgent, IRIS Elements Tax & Accounts, BrightPay. This list is not exhaustive. If you need more information, contact Jon Sharpe.

Transfers of personal data outside the EEA

We use servers in the UK/EEA to process your personal data.

However, there may be occasions when we may have to use, or our third party suppliers use, services that host your information outside the United Kingdom or European Union or other approved countries. When this occurs, we will use reputable suppliers that have gone through information security due diligence, have contractual clauses about the required standard of data processing, and meet legally approved requirements that your information is looked after to a standard as if it were in the UK. For more information about this please contact us using the Contact Us section below.

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 of our records relating to you as follows:

- where tax returns have been prepared it is our policy to retain information for 7 years from the end of the tax year to which the information relates.
- where ad hoc advisory work has been undertaken it is our policy to retain information for 7 years from the date the business relationship ceased.
- where we have an ongoing client relationship, data which is needed for more than one year's tax compliance (e.g. capital gains base costs and claims and elections submitted to HMRC) is retained throughout the period of the relationship, but will be deleted 7 years after the end of the business relationship unless your employer as our client ask us to retain it for a longer period or there is some other legal hold on the data.

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 and this will be supplied in the form agreed between us. Documents and records relevant to your employer's tax affairs are required by law to be retained as follows:

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 3 years at the termination of the contract.

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 Jon Sharpe.

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:

- 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 unless your requests become too frequent or are too extensive or are made for reasons other than a genuine request for your data.

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). 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). 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).

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.

Contact Us

If you have requested details of the information we hold about you and you are not satisfied with our response, or you think we have not complied with the GDPR or DPA 2018 in some other way, you can contact us at jonsharpe@adminrescue.co.uk.

If you are not satisfied with our response, you have a right to lodge a complaint with the ICO (www.ico.org.uk).

Last update March 2024