Data Privacy Policy

This Data Privacy Policy applies to all activities whereby JR Accounts are a Data Processor and/or a Joint Data Controller with a Data Controller in relation to Personal Data as defined by the GDPR.

Company Details

1. This Policy applies to JR Accounts. Any references to 'we', 'us' or 'our' in this Policy refers to JR Accounts and any of the employees/contractors hired by us.

2. JR Accounts is the trading name of J.R. Accounts Compilations Limited, registered at Companies House with registration number 03548223.

3. Our principal address is 164-166 High Road, Ilford, Essex, IG1 1LL.

Purpose of this Policy

4. The purpose of this Policy is to explain how we collect and use Personal Data as a business and in connection with the Services we provide to Clients and Data Subjects and their Rights with regards to this Personal Data.

5. We are committed to protecting the confidentiality and privacy of any Personal Data and this Policy will be updated periodically in line with Data Protection Laws. Please visit our website regularly to stay informed of any changes to this Policy and your Data Protection Rights.

Definitions

6. In this Policy, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

   (a) **'Applicable Laws'** means

      (i) European Union or Member State laws with respect to any Personal Data that is subject to EU Data Protection Laws; and

      (ii) any other applicable law with respect to any Personal Data that is subject to any other Data Protection Laws.

   (b) **'Client'** means the party we are instructed to provide services for, including any entity that owns or controls, is owned or controlled by or is or under common control or ownership with a Client, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise. Clients are either Data Controllers, Data Subjects or both.

(c) **'Personal Data'** means any data which relates to a living individual who can be identified from said data or from said data and other information which is in the possession of, or is likely to come into the possession of, us or any Data Controller and includes any expression of opinion about the individual and any indication of the intentions of us, the Data Controller or any other person in respect of the individual. Personal Data can also include online profiles based on interaction with us, our website and other applications, including Internet Protocol (IP) addresses.

(d) **'Data Controller'** means 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 is, or will be, Processed. The Data Controller will be either a Client or a Data Subject.

(e) **Data Subject'** means the living individual to whom Personal Data relates to. This can be either the Client or any individual for whom the Client is a Data Controller. A Data Subject can also be any potential Clients and any visitors to our website.

(f) **'Joint Data Controller'** means JR Accounts when they are considered a Data Controller of any Personal Data in common with a Client or Data Subject.

(g) **'Processor'** means the Data Processor, JR Accounts.

(h) **'Processing'** means any activities carried out by a Data Controller with Personal Data in relation to obtaining, recording or holding the data or carrying out any operation or set of operations on the information or data, including:-

(i) organisation, adaptation or alteration of the information or data,

(ii) retrieval, consultation or use of the information or data,

(iii) disclosure of the information or data by transmission, dissemination or otherwise making available, or

(iv) alignment, combination, blocking, erasure or destruction of the information or data.

For the purposes of this Policy, when referring to a Processor, we only refer to JR Accounts, not any other Data Controllers.

(i) **'Data Protection Laws'** means EU Data Protection Laws and where applicable, the data protection or privacy laws of any other country.

(j) **'EU Data Protection Laws'** means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR.

(k) **'GDPR'** means EU General Data Protection Regulation 2016/679.

(l) **'Restricted Transfer'** means a transfer of Personal Data from a Client or a Data Subject to JR Accounts; or an onward transfer of Personal Data from JR Accounts to a Sub-Processor, or another Processor contracted by a Client or a Data Subject, where such transfers would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws).

(m) **'Services'** means the Services and other activities to be supplied to, or carried out by or on behalf of JR Accounts, as instructed by a Client or a Data Subject. A full list of the Services we provide can be found on our website.

(n) **'Sub-Processor'** means any person or Processor, (excluding an employee of JR Accounts or any of its contractors) appointed by a Client or a Data Subject or JR Accounts to Process Personal Data in connection with the Services provided.

(o) **'Third Party'** means any Third Party, or Processor, (excluding an employee of JR Accounts or any of its contractors) appointed by a Client or a Data Subject or JR Accounts who has access to Personal Data.

(p) **'Legal/Supervisory/Regulatory Authority'** means any public authority or government agency responsible for exercising autonomous authority over some area of human activity in a regulatory or supervisory capacity. This includes the Information Commissioner's Office, ACCA, HMRC and any Law Enforcement Agencies.

(q) The terms **'Member State'**, **'Personal Data Breach'** and **'Special Categories'** have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

(r) The word **'include'** shall be construed to mean include without limitation and cognate terms shall be construed accordingly.

Authority and Personnel

7. We will take reasonable steps to ensure the reliability of any employee, agent or contractor who may have access to Personal Data.

8. We will ensure in each case that access to Personal Data is strictly limited to those individuals who need to know/access the relevant Personal Data, as strictly necessary for the purposes of providing the agreed Services, and to comply with Applicable Laws in the context of that individual's duties.

9. We will ensure that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

Collection of Personal Data

10. We will collect Personal Data necessary to provision of our Services to our Client.

11. We ask our Clients to only share Personal Data where it is strictly needed for the Services we are providing.

12. Personal Data is made up of all the financial and personal information we collect and hold about Clients, Data Subjects and/or their businesses.

13. Personal Data can be obtained directly from Clients and Data Subjects during the following scenarios:

    (a) information provided when becoming our Client,

    (b) information provided in order to carry out Services we are providing,

    (c) completing the 'Contact Form' on our website,

    (d) visiting our offices and completing our 'Enquiry Form',

    (e) business cards given to us,

    (f) marketing correspondence sent to us.

14. We may have obtained Personal Data indirectly from sources such as:

    (a) social media and networking sites (e.g. Facebook or LinkedIn),

    (b) public sources and internet search engines (e.g. Companies House or Google),

    (c) from Data Controllers providing us with your Personal Data so that we can carry out Services for them (e.g. an employer providing us details so that we can provide Payroll Services to them),

    (d) referrals from our Clients and other business associates,

    (e) recruitment agencies,

    (f) former employers,

    (g) government agencies,

    (h) the technology used to access our Services (e.g. a telephone number from our caller ID, or an IP address from browsing our website),

    (i) other Third Parties instructed by a Data Subject (e.g. a mortgage broker who is requesting an Accountant's Reference).

Categories of Personal Data

15. Personal Data includes, but is not limited to, the following:

    (a) Contact details,

(b) Business activities,

(c) Income, taxation and other financial details,

(d) Professional details (e.g. professional qualifications or employment history),

(e) Family information,

(f) Copies of Correspondence,

(g) Communications records, such as call recordings, emails, text messages etc.

16. We will not hold Special Categories of Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and genetic or biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, unless such Personal Data is necessary for the purposes of providing Services.

17. We may Process certain Special Categories of Personal Data such as country of residence for tax purposes, sources of wealth, sources of income etc. in order to provide specific Services.

18. We will only Process Special Categories of Personal Data where we have obtained explicit consent from a Data Subject or are otherwise lawfully permitted to do so due to Legal or Regulatory requirements.

19. Where a Client is the Data Controller, we will obtain consent to Process Special Categories of Personal Data from a Data Subject via the Client.

Use of Personal Data

20. Our main use of Personal Data is to enable us to provide Services to our Clients, particularly where we are providing Data Processing Services.

21. We are obliged, under Legal and Regulatory requirements to obtain Personal Data in order to provide our Services.

22. By instructing us in any Services, or by providing us with Personal Data directly, a Data Subject (or a Data Controller on behalf of the Data Subject) is authorising us to use their Personal Data.

23. We will comply with all applicable Data Protection Laws in the Processing of Personal Data.

24. We will not Process Personal Data other than on documented instructions unless permitted by law, particularly in relation to criminal activities, money laundering, fraud, terrorist financing, bribery and corruption. This may involve investigating and gathering information and sharing Personal Data with Legal and Regulatory Authorities.

25. We may also use Personal Data for the following purposes:

    (a) Client Management,

    (b) Due Diligence,

    (c) Quality Control,

    (d) Improving/Expanding our Services,

    (e) Internal Assessments,

    (f) Marketing and Promotion to Existing and Potential Clients (unless a Data Subject has specifically requested that we do not contact them),

    (g) Quotations,

    (h) Invitations to Events,

    (i) Meeting Public Interest Obligations,

    (j) Recruitment,

    (k) Recommendation of Your Services,

    (l) Credit Control/Debt Management,

    (m) General Internal Administration.

Data Storage

26. In order to comply with Legal and Regulatory requirements, we need to create records of the Services we provide. These records may contain Personal Data.

27. Records can be held on a variety of media and in different formats based on the nature of the Services we are providing.

28. Data is stored as follows:

    (a) in physical files, which are only accessible by us;

    (b) electronically on our internal server. Our server is password protected and has sufficient security in place to avoid unauthorised access;

    (c) digitally on desktop-based software where all data is stored internally and is protected by our internal security systems;

    (d) digitally on cloud-based software where data is stored externally but is encrypted and is only accessible with the appropriate login details.

29. We currently use the following software:

    (a) Digita – for practise management and marketing purposes,

    (b) Qtac Payroll Bureau and Moneysoft Payroll Manager – for payroll processing services,

    (c) Sage, Iris, TaxCalc, Xero and QuickBooks – for accountancy and book-keeping services,

    (d) LEAP and Perfect Books – for book-keeping for solicitors,

    (e) Microsoft Office – for basic book-keeping and general administration and communications,

    (f) Adobe Acrobat Pro DC – for viewing and password protecting pdf files,

    (g) 7-Zip – for compressing and password protecting Personal Data,

    (h) Dropbox – for sharing data with Clients,

    (i) TeamViewer – to remotely access information on behalf of Clients.

Sub-Processing

30. With written authorisation, we may appoint and use Sub-Processors to Process Personal Data.

31. Prior to the appointment of any new Sub-Processor, a written notice will be issued to the Data Controller, including full details of the Personal Data the Sub-Processor will have access to and the Services they will be providing.

32. If, within 14 days of receipt of that notice, the Data Controller notifies us in writing of any objections (on reasonable grounds) to the proposed appointment, we will not appoint (or disclose any Personal Data to) that proposed Sub-Processor until reasonable steps have been taken to address the objections raised and the Data Controller has been provided with a written explanation of the steps taken.

33. With respect to each Sub-Processor we instruct, we shall:

    (a) carry out adequate due diligence to ensure that the Sub-Processor is capable of providing the level of protection for Personal Data as required by Data Protection Laws before the Sub-Processor processes any Personal Data,

    (b) ensure there are appropriate security measures in place to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the Services involve the transmission of data over a network, and against all other unlawful forms of Processing,

(c) ensure that the arrangement between us and the Sub-Processor is governed by a written contract including terms which offer at least the same level of protection for Personal Data as those set out in this Policy and meet the requirements of the GDPR;

(d) provide Data Controllers with copies of said contracts with Sub-Processors for review if requested,

34. Where the Sub-Processor has been instructed by a Data Controller, we will not be responsible for ensuring compliance with Data Protection Laws by the Sub-Processor.

Sharing Data with Third Parties

35. Occasionally, Personal Data may be accessed by trusted Third Parties for the following purposes:

(a) IT Support

(b) Software Support

(c) Insurers

(d) Financial Service Providers

(e) Professional Advisors

(f) Marketing Service Providers

36. We will ensure that any Third Party we use is capable of protecting Personal Data under Data Protection Laws.

37. We will not share Personal Data with anyone outside of JR Accounts, our Sub-Processors and Third Parties unless:

(a) we have your permission,

(b) we are required to do so in order to provide a Service that has been requested by you,

(c) we are required or permitted by Legal or Regulatory Authorities to do so.

38. We will not be responsible for any Third Parties that gain access to Personal Data as a result of instructions from a Data Controller or a Data Subject.

Restricted Transfers

39. Personal Data may be Processed, transferred to and stored by Sub-Processors and Third Parties to any country or territory as reasonably necessary for the provision of the Services we have been instructed to provide.

40. To allow any relevant Restricted Transfers to take place without breach of applicable Data Protection Law, we agree and warrant:

    (a) that the Processing, including the transfer itself, of the Personal Data has been and will continue to be carried out in accordance with the relevant provisions of the applicable Data Protection Law (and where applicable, has been notified to the relevant authorities of the Member State where the Sub-Processor or Third Party is established) and does not violate the relevant provisions of that State;

    (b) that, if the transfer involves a Special Category of Data, the Data Subject has been informed or will be informed before, or as soon as possible after, the transfer that it's Personal Data could be transmitted to a third country not providing adequate protection;

    (c) that we will follow the procedures set out in this Policy as relates to Sub-Processors and Third Parties.

41. The provisions relating to aspects of Data Protection Laws for Sub-Processing and Third Parties shall be governed by the Data Protection Laws in which the Processor is established.

Retention of Personal Data

42. We retain Personal Data for the following reasons:

    (a) in order to carry out specific Services,

    (b) for Legal and Regulatory requirements,

    (c) marketing and promotion.

43. We will retain Personal Data to the extent and for the period as required by Legal and Regulatory regulations and always provided that the we can ensure the confidentiality of all such Personal Data. We will ensure that such Personal Data is only Processed as necessary for the purpose(s) specified above.

44. We will delete all Personal Data either when it is no longer required or after seven years, whichever is sooner.

45. Personal Data will be disposed of in a secure manner.

46. A written request can be submitted by a Data Controller to us for the:

    (a) return of a complete copy of all Personal Data held by us by secure file transfer in such a format as is considered reasonable,

    (b) deletion and/or to request the deletion of all other copies of Personal Data held by any Sub-Processor or Third Party.

47. We will comply with any such written request if permitted to do so by Legal and Regulatory requirements and provided complying with the request will not hinder any Services we are providing to our Clients.

Data Subject Rights

48. Under Data Protection Regulations, Data Subjects have certain Rights regarding their Personal Data. These are as follows:

    (a) Access – the Data Subject has a Right to verify and access the Personal Data we hold. This information can be requested from us in writing.

    (b) Rectification/Correction – the Data Subject has a Right to update or correct any Personal Data they believe is inaccurate.

    (c) Erasure – the Data Subject can request that their Personal Data is deleted after withdrawing their consent to Processing the Personal Data or when it is no longer required for the purpose for which is was originally obtained.

    (d) Processing Restrictions – the Data Subject can request that the Processing of their Personal Data is temporarily restricted if they believe the Personal Data to be inaccurate, no longer required or wish for the Personal Data to be held rather than erased.

    (e) Portability – the Data Subject can request their Personal Data in a portable format where technically feasible to be sent to themselves or to a Third Party on their behalf.

    (f) Objection – the Data Subject has a Right to object to us Processing any Personal Data unless we can demonstrate compelling and legitimate grounds for the Processing, which may override the Data Subject's own interests or where we need to Process the Data Subject's information to investigate potential fraud or illicit/unlawful activities.

    (g) Automated Individual Decision Making – the Data Subject has a Right to object to the use of any Personal Data for direct marketing purposes, including profiling of the Data Subject for direct marketing purposes. The Data Subject also has the Right to request a review of decisions made based on automated processing that have legal consequences or cause them concern.

    (h) Right to Withdraw Consent – the Data Subject has a Right to withdraw consent at any time for the Processing of any Personal Data where consent is required. This may restrict the Services we are able to provide. Consent will always be requested from the Data Controller/Subject as and when required.

49. Before exercising any Rights, we may need the Data Subject to confirm their identity to ensure Personal Data remains protected.

50. We may be unable to comply with the request of a Data Subject based on Legal and Regulatory Requirements. In cases where the Data Subject is not the Data Controller,

and we are the Joint Data Controller or the Data Processor, we may need written agreement from the Data Controller before we are able to assist the Data Subject in exercising their Rights.

51. We will assist our Clients to fulfil any requests they receive from a Data Subject to exercise their Rights.

52. We shall promptly notify our Client if we receive a request from a Data Subject under any Data Protection Law in respect of Personal Data.

53. We reserve the right to recover any costs incurred when dealing with Data Subject Rights from either our Client or from the Data Subject if the request is excessive or unsubstantiated.

Impact Assessment and Audit Rights

54. We shall make available, on request, all information necessary to demonstrate compliance with this Policy, and shall allow for and contribute to audits, including inspections, by the Data Controller or an auditor appointed by the Data Controller.

55. The Data Controller or it's appointed auditor should give the us reasonable notice of any audit or inspection to be conducted and should make reasonable endeavours to avoid causing (or, if it cannot be avoided, to minimise) any damage, injury or disruption to our premises, equipment, personnel and business during the course of such an audit or inspection.

56. We will provide the Data Controller with reasonable assistance if needed to deal with Data Protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which can reasonably be considered to be a requirement of the GDPR or equivalent provisions of any other Data Protection Laws.

Security

57. Taking into account the nature, scope, context and purposes of your Personal Data, we will implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk involved in being a Joint Data Controller or a Data Processor.

58. We will take measures aimed at protecting Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where Personal Data is transmitted over a network.

59. Security measures include:

    (a) encryption, password protection and internet security to protect electronic data,

    (b) back-up systems to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident,

(c) limiting access to Personal Data to only those that need it,

(d) adherence to the ACCA Code of Ethics and Conduct to ensure that any natural person acting under our authority who has access to Personal Data does not Process this Personal Data except on instructions from a Data Controller, unless he or she is required to do so by the ACCA Code of Ethics and Conduct or by UK law,

(e) destruction of Personal Data that is no longer required,

(f) ensuring the ongoing confidentiality, integrity, availability and resilience of internal systems and those of Sub-Processors and Third Parties.

Personal Data Breach

60. We will notify, without undue delay, the Data Controller of any Personal Data Breach. We will also provide the Data Controller with sufficient information to allow them to meet any obligations to report or inform the Information Commissioner's Office and Data Subjects of the Personal Data Breach under Data Protection Laws.

61. If we are the Joint Data Controller, we will meet any obligations to report or inform the Information Commissioner's Office and Data Subjects of the Personal Data Breach under Data Protection Laws.

62. Notifications of a Personal Data Breach shall as a minimum:

    (a) describe the nature of the Personal Data Breach, the categories and numbers of Data Subjects concerned, and the categories and numbers of Personal Data records concerned;

    (b) describe the likely consequences of the Personal Data Breach; and

    (c) describe the measures taken or proposed to be taken to address the Personal Data Breach.

63. We shall co-operate with the Data Controller to take reasonable steps to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

Governing Law and Jjurisdiction

64. This Policy is governed by the laws of England and Wales.

Cookies

65. Our websites may use cookies to collect Personal Data. Where cookies are used, a statement will be sent to your browser explaining the use of cookies. To learn more, please refer to our Cookie Policy which can be found on our website.

Severance

66. Should any provision of this Policy be invalid or unenforceable, then the remainder of this Policy shall remain valid and in force. The invalid or unenforceable provision shall be either:

    (a) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible,

    (b) construed in a manner as if the invalid or unenforceable part had never been contained therein.

Liability

67. Any person who has suffered material or non-material damage as a result of an infringement of Data Protection Regulations shall only have the right to receive compensation from us for the damage suffered if the damage has occurred as a result of us failing to fulfil our Data Protection obligations.

68. If the damage is a result of any Sub-Processor or Third Party instructed by us, compensation should be sought from said Sub-Processor or Third Party.

69. Our liability for direct losses that arise shall not exceed the aggregate amount of the fees the Data Controller has paid to us for Processing Services in the last three months preceding the event.

70. We shall be exempt from liability if it proves that we are not in any way responsible for the event giving rise to the damage.

71. Where we have paid full compensation for the damage suffered, we will be entitled to claim back from the Data Controller, if it was involved in the same Processing, that part of the compensation corresponding to the Data Controller's involvement in the damage.

72. If we are found by any Supervisory Authority (such as the Information Commissioner's Office) to have acted negligently, or to have wilfully contributed to a data breach/loss over data for which we were responsible, and this has compromised the Data of a Subject, we will be held accountable by the Supervisory Authority.

Changes

73. This Policy has been updated on 25 May 2018.

74. This Policy is subject to change and the most up-to-date version of this Policy is available on our website.

75. A Data Controller or a Data Subject may propose variations to this Policy which they consider to be reasonable and necessary to address the requirements of any Data Protection Law. This must be done within 30 days from the date the Policy is updated.

76. If a Client is in disagreement with this Policy and we cannot agree on proposed variations, we may not be able to continue providing our Services to them

Queries and Complaints

77. If you have any queries regarding this Policy or if you have any concerns regarding your Personal Data, our contact details can be found on our website.

78. If we are unable to deal with your queries or concerns, you can contact the Information Commissioner's Office. Their details can be found on https://ico.org.uk/.