MENZIES
BRIGHTER THINKING

PRIVACY NOTICE

Last reviewed: 22 March 2024

Contents

1. Summary

1.1. Menzies LLP, Menzies Corporate Finance Limited and Menzies Wealth Management Limited are registered as Data Controllers with the Information Commissioner's Office, as are the following individual insolvency practitioners, who are licensed by the Insolvency Practitioners Association:

- Bethan Evans
- Freddy Khalastchi
- John Cullen
- Jonathan Bass
- Laurence Pagden

- Giuseppe Parla
- Rachel Lai
- Simon Underwood

Collectively we will refer to them as 'Menzies', 'we', 'us' and 'our' in this policy.

1.2. This Privacy notice explains:

- what information we gather about you
- how we obtain that information
- what we use that information for
- who we give that information to
- how long we retain that information
- your rights in relation to your information
- who you can contact for more information or in relation to any queries that you may have.

2. Scope

2.1. This policy applies to individuals whose data we process except:

- clients and contacts of Menzies Wealth Management, who should refer to the Menzies Wealth Management Limited Privacy Notice at www.menzies.co.uk/legal. Where you have contact with 0Menzies LLP and/or its other subsidiaries as well as Menzies Wealth Management Limited, both Privacy Notices may apply;
- our employees, who should refer to the Workplace Privacy Notice in the employee handbook;
- recruitment candidates, who will be issued with a privacy notice at the point of collecting their data.

3. Definitions

Personal data means any information relating to an identified or identifiable person ('data subject') such as a name, postal/email address, telephone number or identification number.

Special categories of personal data mean personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, 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 and data concerning criminal convictions or offences

Data subject means any living individual who is the subject of personal data held by Menzies. Where this policy refers to 'you' or 'your', we are referring to the relevant data subject.

Processing means any use of personal data such as the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, dissemination, erasure and destruction.

Data controller means the organisation which decides the purposes and means of the processing of personal data

Data processor means an individual or organisation that processes personal data on behalf of a data controller

Consent means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Staff means anyone working at or for us on a permanent or temporary basis, including Partners and permanent, interim and temporary employees, trainees and interns.

4. Principles of data protection

4.1. Personal data shall be:

- processed lawfully, fairly and in a transparent manner
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation')
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')

- accurate and, where necessary, kept up to date ('accuracy')
- kept for no longer than is necessary ('storage limitation')
- 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 ('integrity and confidentiality').

5. Data controller

5.1. We will usually be a data controller in relation to the data that we process; however, for some services, such as Payroll and Business Outsourcing, we will be a processor. In relation to a formal insolvency appointment, a Company or debtor may be subject to an insolvency process ("each referred to as "insolvency"). Where Menzies insolvency practitioners are appointed (i.e. acting as an "insolvency officeholder"):

- they act in the capacity of agents of the Company or debtor in fulfilling the role of managing the Company's or debtor's affairs, business and property and so the Company or debtor continues to be the data controller for personal data collected and processed in this context; and
- they act as separate data controllers where they process data to comply with their own legal and regulatory requirements as insolvency practitioners.

6. What information we collect about you

6.1. The information we collect will depend on the reason we are collecting it and the nature of our relationship with you. It is our policy to collect only the minimum information required from you. If you believe we have collected excessive information about you, please contact us by the means indicated in the **Contact us** section below to raise any concerns you may have.

6.2. Where we need to collect personal data in relation to providing our services, we ask you to provide us with only the data that we have requested.

6.3. Although you do not have to provide any of your personal information to us, if we ask you to do so and you refuse, we may be unable to provide you with the information, goods or services you want from us.

6.4. When providing us with other data subjects' information, such as your family or your employees, you must ensure you have a lawful basis for doing so.

6.5. Examples of the personal information we may collect include:

Clients and prospective clients including associated individuals

- name
- contact details including phone, email, address and any other relevant contact details
- personal details such as date of birth, gender, marital status
- financial information including income, taxation, investments, benefits, assets, insolvency records and other financial information relevant to the services we provide
- bank account details, and/or
- Employment details
- Facial recognition data

Business contacts including suppliers and individual contacts at supplier organisations

- name
- contact details including phone, email, address and any other relevant contact details
- employer/associated business name, and/or
- job title.

Our employees, partners and contractors

Menzies employees should refer to the Workplace Privacy Notice in the Employee Handbook for information on how Menzies collect and process employee personal information.

7. How we collect personal information including special category information

7.1. You or others may provide us with your personal information via various means, including:

- the Menzies Client Portal
- direct correspondence with us via meeting, phone, in writing, including by email or fax

- searching and browsing our website(s) for content
- subscribing to or ordering newsletters and/or publications; participating in bulletin boards, discussion or message forums
- responding to surveys
- registering for events and conferences
- submitting resumes or work history information
- contacting us for further information
- visiting our website(s) while logged into a social media platform, and/or
- providing us with business cards or other contact information.

7.2. We currently employ the services of Smart Credit Limited T/A Smart Search, an Anti-Money Laundering (AML) verification service, to assist us with performing identification checks on our clients for the purposes of compliance with the Money Laundering Regulations. Any personal information received from Smart Search will be processed only to confirm your identity to us for the purposes of preventing money laundering or terrorist financing. You can access Smart Search's privacy policy at https://www.smartsearch.com/privacy-policy where you will find more information regarding Smart Search's data processing activities. The information received from Smart Search may include special category information.

8. Special category personal information

8.1. We may ask you to provide special category personal information where required in relation to the services we provide. We ask that you do not provide us with special category personal information unless we have requested it.

9. Our website(s)

9.1. Our website(s) may link to third-party sites not controlled by us and which do not operate under our privacy practices. When you link to third-party sites, our privacy practices no longer apply. We encourage you to review each third-party site's privacy policy before disclosing any personally identifiable information.

10. Cookies

10.1. Please refer to our Cookie Policy at https://www.menzies.co.uk/gdpr-data-protection-legal/

11. Use of personal information

11.1. When you provide personal information to us, we may use it for any of the purposes described in this Privacy Notice or as stated at the point of collection, including:

- to provide our services to you
- to verify your identity
- to administer and manage our website(s), including:
  - to confirm and authenticate your identity and prevent unauthorised access to restricted areas of the site(s)
  - to personalise and enrich your browsing experience by displaying content that is more likely to be relevant and of interest to you
  - to sort and analyse user data (such as determining how many users from the same organisation have subscribed to or are using our websites)
  - to understand how people, use the features and functions of our websites in order to improve the user experience
- to develop our businesses and services
- to market our services to you
- to conduct quality and risk management reviews
- to perform tests and demo systems when assessing solutions to use internally
- to use systems on behalf our clients to deliver our services
- to monitor and enforce compliance with our Terms, including acceptable use policies, and/or
- any other purposes for which you provided the information to us.

11.2. We do not collect personally identifying information for sale

12. Lawful bases for processing personal information

12.1. We rely on one or more of the following processing conditions:

- to perform our contractual obligations to you or
- our legitimate interests in the effective delivery of information and services to you and in the effective and lawful operation of our businesses (provided these do not interfere with your rights)
- to satisfy any legal and regulatory obligations to which we are subject, and/or
- where no other condition for processing is available, if you have agreed to us processing your personal information.

12.2. Further to paragraph 12.1, Menzies insolvency practitioners may process personal data for the purposes of complying with their legal obligations and/or legitimate interests in relation to the insolvency process, which may include:

- realisation of assets
- agreement of claims (including employee claims)
- payment of dividends
- calculation and analysis of payroll
- establishing, exercising or defending legal claims, and/or
- circularising information to creditors, which on occasion includes the names and addresses of employees, customers and creditors of the Company.

13. Security of personal information

13.1. We have implemented generally accepted standards of technology and operational security in order to protect personally identifiable information from loss, misuse, alteration or destruction.

13.2. Only authorised persons are provided access to personally identifiable information we have collected, and such individuals have agreed to maintain the confidentiality of this information.

13.3. Although we use appropriate security measures once we have received your personal data, the transmission of data over the internet (including by e-mail) is never completely secure.

13.4. We endeavour to protect personal data, but we cannot guarantee the security of data transmitted to or by us.

13.5. All our staff undergo data protection training and are required by their employment contracts to adhere to our policies. In addition, many of our staff are members of professional institutes whose codes of conduct must be adhered to. Depending on the staff member's area of expertise, these could include:

- ICAEW Code of Ethics
- FCA Code of Conduct, and/or
- Insolvency Code of Ethics

14. Sharing personal information

14.1. We may transfer, share or disclose the personal data we collect from you to third parties (and their respective subcontractors, and/or their subsidiaries and affiliates) for:

- the purposes for which the information has been submitted
- the purposes listed above under the **Use of personal information** section
- the administration and maintenance of our website(s) and/or
- other internal or administrative purposes.

14.2. We also may transfer, share or disclose personal data to third party service providers such as:

- government agencies such as HM Revenue and Customs and Companies House
- organisations who provide marketing services such as telesales on our behalf
- our regulating bodies
- members of the HLB International network
- other professional service providers such as accountants and solicitors
- credit reference and fraud prevention agencies
- document security and storage services
- network infrastructure providers
- website hosting and management services
- data analysis providers
- data backup providers

- our insurers
- banks and other financial institutions
- debt recovery agencies
- payment service providers
- law enforcement agencies
- business consultants such as those auditing our business systems
- cyber security consultants
- building management and security agents
- life insurance and pension providers, and/or
- social media sites.

14.3. The third-party providers may use their own third-party subcontractors that have access to personal data (sub-processors). It is our policy to use only third-party providers that are bound to maintain appropriate levels of security and confidentiality, to process personal information only as instructed by us, and to flow those same obligations down to their sub-processors.

14.4. We may share your personal data between the controllers listed at the beginning of this policy where we have a legitimate reason to do so given the service(s) we are providing, and the lawful basis and purpose of the processing.

14.5. A list of the data processors that we routinely use in the course of running our business can be found on our website at https://www.menzies.co.uk/gdpr-data-protection-legal/ .

15. International transfers of personal information

15.1. Your personal information may be transferred to and stored outside the country where you are located. This includes countries outside the UK or European Economic Area (EEA) and countries that do not have laws that provide specific protection for personal information.

15.2. Where we collect your personal information within the UK / EEA, transfer outside the UK / EEA will be only:

- to you
- to a recipient located in a country which provides an adequate level of protection for your personal information, and/or
- under an agreement which satisfies UK requirements for the transfer of personal data to data processors or data controllers outside the UK and EEA, e.g. International Data Transfer Agreement clauses or,
- in exceptional circumstances only, with your explicit consent.

16. Other disclosures

16.1. We may also disclose personal information to third parties under the following circumstances:

- when explicitly requested by you
- when required to deliver publications or reference materials as requested by you
- when required to facilitate conferences or events hosted by a third party
- for regulatory compliance purposes, and/or
- as otherwise set out in this Privacy Notice.

16.2. We may also disclose your personal information to law enforcement, regulatory and other government agencies and to professional bodies and other third parties, as required by and/or in accordance with applicable law or regulation. This includes disclosures outside the country where you are located.

17. Retention of personal information

17.1. We will destroy correspondence and other files that we store electronically or otherwise once we deem these to be no longer relevant except those that are required by law or professional guidelines to be kept for specified periods. Unless we are required to keep data for specified periods, we will typically keep it for no longer than seven years.

18. Disposal and destruction

18.1. When the retention periods expire we shall dispose of and destroy all personal data unless a Partner or Director authorises that such data should be retained.

18.2. Any personal data recorded on paper, which does not need to be retained on file, shall be shred or deposited to the document security bins located within each office.

18.3. Historic paper files are stored at specialist document storage facilities. Any paper file retrieved from archive shall be returned to archive as soon as the need has been fulfilled. If the data on the file is past its retention period at the point that the file is no longer required then the file shall be shred or disposed of in the office document security bins.

18.4. The office document security bins are emptied periodically by document disposal providers.

18.5. Files held in archive are securely disposed of periodically by the facility in accordance with the catalogued retention periods.

18.6. Unless filed in a permanent file or in other such way as to indicate a specified retention period, digital data will be automatically deleted after 7 years.

19. Marketing

19.1. We keep contact information (such as mailing list information) until a user unsubscribes or requests that we delete that information.

19.2. Where we are legally required to obtain your explicit consent to provide you with marketing materials, we will only provide you with such marketing materials if you have provided consent for us to do so.

19.3. If you opt into any subscriptions, you will receive automated emails when content is updated. If you opt into any newsletters, you will receive curated emails known as newsletters. If you select any preferences such as issues, topics, subjects or industries, you may receive email communications related to those self-selected topics.

19.4. If you want to unsubscribe from mailing lists or any subscriptions, you should look for and follow the instructions we have provided in the relevant communications to you. Alternatively, you can at any time contact us to request that such communications cease.

19.5. If you choose to unsubscribe from any or all mailings, we may retain information sufficient to identify you so that we can honour your request.

20. Rights in relation to your information

20.1. You have certain rights in relation to the personal information we hold about you. In particular, you have the right to:

- request a copy of personal information we hold about you
- ask that we update the personal information we hold about you, or correct such personal information that you think is incorrect or incomplete
- ask that we delete personal information that we hold about you, or restrict the way in which we use such personal information
- object to our processing of your personal information, and
- withdraw your consent to our processing of your personal information (to the extent such processing is based on consent and consent is the only permissible basis for processing).

20.2. If you would like to exercise these rights or understand whether these rights apply to you, please contact us via the means listed in the **Contact us** section of this notice.

21. Automated decision making

21.1. We will not use your personal information for automated decision making.

22. Roles and responsibilities

22.1. The Management Committee of Menzies has ultimate responsibility for ensuring compliance with the GDPR, the data protection principles and this policy.

22.2. The day-to-day operational responsibility for ensuring Menzies complies with the GDPR, the data protection principles and this policy lies with the firm's internal Data Protection Representative (DPR). Menzies' Risk and Compliance Senior Manager is the currently appointed DPR and can be contacted at dataprotection@menzies.co.uk or on 0330 912 9142.

22.3. All staff have a responsibility to comply with the GDPR, the data protection principles and this policy when carrying out their duties. Line managers are responsible for supporting staff's adherence with this policy. Failure to comply with this policy may result in legal and/or disciplinary action.

23. Changes to this Privacy Notice

23.1. We may update this Privacy Notice at any time by publishing an updated version at https://www.menzies.co.uk/gdpr-data-protection-legal/ . So that you know when we make changes to this Privacy Notice, we will amend the revision date at the top of this page. The new, modified or amended Privacy Notice will apply from that revision date. Therefore, we encourage you to review this Privacy Notice periodically to be informed about how we are protecting your information.

24. Contact us

If you have any questions or complaints about this Privacy Notice or the way your personal information is processed by us, or would like to exercise one of your rights set out above, please contact us by one of the following means:

Form: https://www.menzies.co.uk/contact-us/

Email: dataprotection@menzies.co.uk

Post:
Data Protection Representative
Menzies LLP
Lynton house
7-12 Tavistock Square
London
WC1H 9LT

You also have the right to lodge a complaint with your local data protection regulator, which in the UK is the Information Commissioner's Office (ICO). The ICO can be contacted by the following means:

Form: https://ico.org.uk/global/contact-us/

Telephone: 0303 123 1113 (local rate – calls to this number cost the same as calls to 01 or 02 numbers). If you're calling from outside the UK, please call +44 1625 545 700.

Post:
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF