MacDonald Accountancy Services Limited - Privacy Statement - Clients

This Privacy Statement identifies, how and why we collect and use personal information and what rights you have in relation to the personal information we collect. This is to comply with the General Data Protection Regulations (GDPR) 2018. Your information is important to us and we have systems in place to protect it.

For the purposes of the GDPR, MacDonald Accountancy Services Limited is both a Data Controller and a Data Processor. In whichever role we will ensure that we have procedures and policies in place to keep all information safe and secure. MacDonald Accountancy Services Limited is registered with the Information Commissioner's Office

We will ensure that all our clients have the opportunity to see our Privacy Statement and to consent to the processing of their data in accordance with it.

MacDonald Accountancy Services Limited can be contacted at 6-10 Glasgow Road, Bathgate, West Lothian, EH48 2AA. The Data Protection officer is Ms P MacDonald who can be emailed on info@macasltd.com.

Personal data is information that relates to a person who can be identified directly from the data or who can be identified indirectly from the data in combination with other information.

The GDPR applies when Personal Data is processed by automated means or manually where it is part of a filing system.

The GDPR introduced 7 principles in connection with how data is processed:

1 principle of lawfulness, fairness and transparency
2 principle of purpose limitation
3 principle of data minimisation
4 principle of accuracy
5 principle of storage limitation
6 principle of integrity and confidentiality
7 principle of accountability

The GDPR also includes provisions concerning your rights and issues to do with transferring data outside of the European Economic Area.

What types of Personal Data do we collect?

This list is not exhaustive but indicative.

We collect identity data such as name; address; date of birth and photo id such as driving licenses or passports.

We collect contact details such as phone numbers and emails for you and your business.

We collect your web address and details of facebook/twitter accounts.

We collect bank account details and savings and pension details.

We collect HMRC generated reference numbers, for example National Insurance Numbers, Unique Tax Reference numbers, VAT, PAYE and CIS deduction reference numbers.

We collect business information, for example invoices, raised by you or invoices made out to you and correspondence between yourself and various third parties, together with loan and finance agreements, share certificates and dividend information and letters which may be addressed to you from a variety of sources.

We collect payroll information.

We also collect historic tax and accounting data, for example, from before you became a client of ours.

We have access to your information via HMRC portals and cloud-based software.

Special Categories of Personal Data – as classified under the GDPR

The only special category of personal data we collect is your Ethnic Origin. We do not collect the following special categories: Race; political opinions; religious beliefs; trade union membership; genetic data; biometric data; health data; data concerning sex life or sexual orientation.

What is the lawful basis on which we process personal data?

Under GDPR, there are 6 bases for lawful processing

1 Consent
2 Contract
3 Legal obligation
4 Vital interests
5 Public task – ie in the Public Interest or for official functions (with basis in law)
6 Legitimate interests (processing is necessary for our legitimate interest or for that of a third party)

Our main lawful bases are under Consent, Contract or legitimate interests. In certain circumstances, such as to comply with Anti-Money Laundering legislation, we would have Legal Obligation as the basis for lawful processing.

We establish consent with all our clients as a positive opt in which is explicit. Our engagement letter constitutes our contract and we obtain authorisation to act as agents with HMRC via form 64-8 and the use of specific authorisation codes from HMRC. We also have consents in place for information sharing via cloud-based software.

We process personal data as we are required to do to meet professional standards and legal requirements and to fulfil our contract with you and manage our business.

We process personal data via data analytics to improve our website; products/services and marketing.

We consider how the processing may affect the individual concerned and would only process data in ways that would be expected unless, if unexpected, that processing is justified. We do not deceive or mislead people when we collect their personal data.

We do not do anything generally unlawful with personal data or which would cause a breach of a duty of confidence. Our organisation would not exceed its legal powers or exercise those powers improperly. We would not infringe copyright or breach an enforceable contractual agreement or an industry-specific rule or the Human Rights Act 1998.

Whose personal data do we collect?

In order to carry out our duties, we handle personal data from:

- Our clients,
- Company directors/partners
- Family members of our clients
- Business associates/suppliers/customers/employees of our clients
- Other advisors of our clients.

(This list is not exhaustive, but indicative).

Children

Our services are directed primarily at adults, but we may process data concerning children under 18 years of age if they are related to our clients or are employed by our clients. We are aware that only children who are aged 13 or over are able to provide their own consent as our lawful basis for processing. For children younger than 13 years old, an adult holding parental responsibility would need to consent on their behalf.

Should we provide services or process data concerning children, we will ensure that those children or their parents/guardians, understand their rights under the GDPR.

How do we collect your personal information?

We collect personal information primarily from you, but we may also obtain information from our Anti-Money Laundering compliance software – Credit Safe. This will identify issues concerning identity or International criminal activity. We also collect personal information via HMRC portals, following your authorisation and via cloud-based software to which you have given us access and to which you have uploaded personal data. We also obtain personal data from other professional advisors to whom you have granted us access.

We will primarily list personal information on our Information Sheet and we will initially obtain copies of photographic ID from you.

We will also record information you give us via telephone calls, emails or letters.

How do we use your personal information?

We are required by the GDPR to be clear as to why we use your personal information and not to use it in a manner which is incompatible with those purposes. In summary we would use your personal information for the following purposes:

1 To provide you with the services we have contracted to provide
2 To comply with legal obligations in respect of fraud and money laundering
3 For financial management and debt recovery

4 To market services and events
5 To administer payments from you.

We will ensure the personal data we process is adequate, relevant and limited to what is necessary in relation to the identified purposes.

We will also ensure that we take all reasonable steps to ensure that the personal data we hold is up to date and accurate.

Data sharing

We share data with staff in our organisation as is appropriate. If you request that some information is restricted to certain individuals only we will do everything in our power to honour that request.

We share data with your consent with HMRC, financial institutions, other individuals or agencies and we would share data without your consent with the Financial Conduct Authority if we had suspicion of money laundering or terrorist activities. In certain other circumstances for example under a Court Order or in connection with a police investigation, we may be required by law to disclose information. We would seek your consent unless we were legally prohibited from so doing.

We may also share your data with other professional advisors with your specific consent and on a "need to know" basis. We would only share the specific information relevant to the particular advice.

We do allow access to our IT systems by our IT service providers and our other software and Cloud based software providers. Data including your personal data can be stored on Cloud based software and is then accessible by those service providers, either routinely or in the situation of assisting with a technical issue.

The IT service providers we use and the software providers we use are all required to adhere to the GDPR and in choosing them one of our criteria is that they do have policies in place which are compliant.

We would also seek your consent for us to employ the use of software services.

We are required as a small practice to have an arrangement with an Alternate Firm under which should anything happen to key personnel which would prevent them from working to safeguard the business and client data, the Alternate Firm would step in. The Alternate Firm would adhere to contract law and would be under a professional duty to continue the services of MacDonald Accountancy Services Limited without interruption. Clients would be advised of this situation. The Alternate Firm would be a suitably qualified firm with suitable adherence to GDPR. They would however, have access to client data on the same basis as set out in this statement.

Should a situation ever arise whereby the practice were to be sold, a new firm may seek consents from clients to act on their behalf. All clients would be notified in advance of any such change.

We do not use bureaux to process data on our behalf and currently all data processing is completed in-house. We may from time to time use sub-contractors to carry out specific pieces of work which may require those sub-contractors to have access to personal data. In this instance we would ensure that those sub-contractors had Data Protection policies in place and had signed a non-disclosure agreement

and contract with ourselves such that they would not breach our own policies as set out in this Privacy Statement.

How long do we retain your personal information?

We will not keep personal data any longer than we need it and will periodically review and erase or anonymise data which we are no longer required to keep.

We are required by professional standards to keep data in connection with work we have carried out for a period of 8 years and either ourselves or our clients are required to keep information supporting tax returns/VAT returns/employer records for up to 6 years. Data may need to be kept for longer in order to preserve records in case of an HMRC investigation on the grounds of suspected fraud.

We will keep original documents in our offices or at a secure storage facility, or we will arrange for our clients to retain their own records after three years have elapsed. We will only destroy records which we think are not required, after 8 years. If there are long term implications – for example with purchase agreements, clawback relief, elections, we will keep records on our system for longer than 8 years. We may also keep electronic historic accounting records for the entire period of our client's tenure with us.

Should a client leave, we can return original documents to that client, or with permission to a new advisor, but we are required to retain copies and our own working papers for a period of 8 years following the completion of the work. If a client has left, we will destroy both paper and electronic records on a rolling basis subsequently.

Data Security

We employ reputable IT service providers to assist us with our IT services.

We ensure that if we use software or cloud-based systems that those providers have a suitable policy in place in compliance with GDPR.

We are currently going through a recognised Cyber-security accreditation process.

We have secure back up facilities and procedures which ensure that all our data is backed up each night to a secure off-site facility.

Our in -house office computers are protected by encryption and virus and malware protection.

Any off-site access to client files would only be carried out via a VPN link.

We have two-step authentication which adds an extra layer of security if we are accessing our email accounts or client information via cloud-based software.

Passwords for computers and our access systems are regularly changed.

Our offices are protected by a burglar alarm system and locks.

All staff are made aware of the firm's duties under GDPR and sign a non-disclosure agreement as part of their employment contract. Similarly so do any sub contractors or third party advisors.

Clients are asked to sign an authorisation to receive emails which may include personal data and are given the option of creating a secure mailbox with two step authentication in place.

Files containing paperwork are locked away at night and are anonymised.

Any paperwork which is to be destroyed is shredded and destroyed securely.

Your rights under GDPR

GDPR provides the following rights for individuals:

1 The right to be informed
2 The right of access
3 The right of rectification
4 The right to erasure
5 The right to restrict processing
6 The right to data portability
7 The right to object
8 Rights in relation to automated decision making and profiling

We do not utilise any systems which involve automated decision making and profiling.

We are aware of these rights and will seek to uphold them. We will inform you about your personal data via our Privacy Statement and will notify you of any significant changes.

We will make our Privacy Statement available via our website and via noticeboards in the office. We will also ensure that individuals have seen the Privacy Statement within one month of our obtaining personal data either directly or from a third party source. If the latter, we are not required to provide the information if the individual already holds it or if to do so would involve a disproportionate effort or if we are required not to disclose the information by law.

Subject access requests

You have the right to obtain a copy of your personal data and any supplementary information. You may also request the purposes of our processing, details of the recipients of any personal data, the retention periods we will employ and the criteria used and information about the source of the personal data and our safeguards.

Rights of rectification/erasure or to restrict processing

You can request that incorrect data which has come to light is corrected.

You can request that restrictions are placed on processing, but we may find that we have legitimate grounds to process the data, which would be advised to you.

You can request that your personal data is erased but if for specific legal or professional reasons we cannot comply we will set out the reasons why within one month.

If a request is manifestly unfounded or excessive we may charge a “reasonable fee” to deal with the request or we may refuse to deal with the request. We would in that instance explain our reasons.

Requesting the transfer of your personal data to you or a third party.

This right extends to information which is automated and which you initially consented for us to use. We will provide your data in a machine readable format to you or a third party you have authorised.

Transferring personal data outside the EU/EEA

MacDonald Accountancy Services Limited will ensure that the data we hold is held within the EU as required by the regulation or by a country deemed to have adequate data protection law by the EU. There are other data protection regimes in places outside the EU and if data were for whatever reason transferred to a non-EU country we would advise you and ensure that we felt the necessary safeguards were in place.

Emails

We cannot guarantee that information sent by email will be protected and if this is a concern please let us know and we can set up an alternative method of communication.

Data breaches

If a data breach comes to light we will in the first instance investigate the matter and evaluate the risk of any personal data having been compromised.

We will correct the situation and notify the individual if we feel that there has been a significant risk. If a serious breach occurred we would notify the Information Commissioner's Office.

Complaints

We would endeavour to resolve any complaints in the first instance and would encourage you to notify us of any concerns you have.

You also have the right to complain to the Information Commissioner's Office directly. The contact details are as follows:

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

Telephone 0303 123 1113 or 01625 545 745

Website: https://ico.org.uk/concerns

We hope that we can resolve any issues and can assure you that our intention is to comply with GDPR and our professional and legal obligations and to ensure the safety and correct processing of your personal data.

We also have a privacy statement containing our procedures for personal data belonging to staff and prospective employees which can be obtained by data subjects by application to info@macasltd.com.