GENERAL DATA PROTECTION REGULATIONS (GDPR) POLICY

Anderson Accountancy (UK) Ltd
33 Taranto Road
Southampton
Hampshire SO16 5PL
Tel. 01794 521 300

Contents

INTRODUCTION

Anderson Accountancy (UK) Ltd (AAUK) is required to collect information about individuals to carry out its functions as a recognised professional accountancy practice and to act in accordance with relevant legislation and regulatory requirements.

In this policy, personal data is defined as 'information which relates to a living individual and from which they can be identified, either directly or indirectly' and this data may be held either electronically, on paper or both. Irrespective of how information is collected, recorded and processed, AAUK ensures that personally-identifiable information is dealt with properly and in compliance with the General Data Protection Regulations (GDPR) as well as any other relevant regulatory requirements or legislation.

In undertaking its business, AAUK creates, gathers, stores and processes data on a variety of subjects such as clients (both current and previous), employees, sub-contractors and suppliers. The use of personal data for clients ranges from personal information and financial transactions throughout the lifetime of their engagement with AAUK and for a duration after the cessation of the engagement as required by legislation and statutory requirements – currently 6 years plus the current year.

The GDPR places obligations on the AAUK and the way it handles personal data to ensure personal data is processed fairly, lawfully and securely. This means that personal data should only be processed if there is a valid condition of processing (e.g. consent obtained from the data subject or it forms part of the legitimate interest of the organisation). There are restrictions on what can be done with personal data such as passing personal information on to third parties, transferring information outside the EU or using it for direct marketing.

PURPOSE OF POLICY

This policy sets out the responsibilities of Anderson Accountancy (UK) Ltd to comply fully with the provisions of the GDPR. This policy applies to all staff and relates to any item of personal data that is created, collected, stored and/or processed through any activity of AAUK.

DATA PROTECTION PRINCIPLES

Anderson Accountancy (UK) Ltd is required to adhere to the six principles of data protection as laid down in the GDPR which means that information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. The six principles are:

1) Personal data shall be processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency').
2) Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in any manner incompatible with those purposes. Further processing for archiving, historical research or statistical purposes is permissible ('purpose limitation')
3) Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed ('data minimisation').
4) Personal data shall be accurate and where necessary kept up to date ('accuracy').
5) Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose ('storage limitation').

6) Personal data shall be processed in a manner that ensures appropriate security including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

PERSONAL DATA

Personal data is information about a living individual, who is identifiable from that information or who could be identified from that information when combined with other data which AAUK either holds or is likely to obtain. GDPR also refers separately to 'special categories' of personal data which includes particularly sensitive personal information such as income and tax liabilities. Further information and guidance on personal data, including how AAUK categorises individuals and the justification for holding and using that data is detailed in Appendix 1.

The definition of 'processing data' includes obtaining/collecting, recording, holding, storing, organising, adapting, aligning, copying, transferring, combining, erasing and destroying the information or data. It also includes carrying out any operation or set of operations on the information or data, including retrieval, consultation, use and disclosure. AAUK remains responsible for the control of personal data it collects even if that data is later passed on to another organisation or is stored on systems or devices owned by other organisations or individuals.

Anderson Accountancy (UK) Ltd does not knowingly collect, use or share information that could reasonably be used to identify children under the age of 16 without prior parental consent or consistent with applicable law.

AAUK collects data in the form of a paper-based client file which records various pieces of information vital for the deliverance of the services contracted under the Letter of Engagement signed by all clients. In all circumstances, personal information relating to sole traders, directors of limited companies, shareholders in companies and trustees of charities is recorded and stored both in paper file and electronically on one or more database systems. The information collected is shown in Appendix 2.

Paper-based data is filed in locked filing cabinets within a locked room outside office hours. Electronic data is stored in one or more computer software packages all of which are password protected and accessed via password protected PC's. The data is stored on a Network Attached Storage device (NAS) which is also password protected and situated behind a firewall. All security measures are taken to protect data as far as is reasonably practical.

Electronic data is regularly backed up to a portable USB hard disk drive which is kept in the secure possession of the Data Protection Officer while off-site. This back up is a direct copy of the data stored on the NAS and is also secured with password protection to prevent unauthorised access if lost or stolen.

With regard to the individual's right to be forgotten (erasure of data), AAUK will comply where is reasonably practical to do so within the guidelines of GDPR but also complying with other legislation and statutory rulings as required. Money Laundering Regulations and HM Revenue and Customs require that certain information is retained for a number of years before erasure is allowed so therefore full compliance with the "right to be forgotten" may not be possible. AAUK will confirm details upon request.

DATA BREACHES

Anderson Accountancy (UK) Ltd employees, past and present, have a contractual obligation to protect AAUK's information assets, systems and infrastructure. They are required at all times, to act in a responsible, professional and security-aware manner and to fully comply with the GDPR and related policies.

Examples of personal data breaches include:

- Loss or theft of data or equipment
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Unauthorised disclosure (e.g. email sent to the incorrect recipient)
- Human error
- Hacking attack

Employees are required to:

- Identify any security shortfall in existing practices.
- Immediately report any software malfunctions, security incidents, suspected viruses, faults, weaknesses or threats, observed or suspected, to AAUK's Data Protection Officer.

All actual or suspected security incidents are reported to AAUK's Data Protection Officer who will undertake the following measures:

- Identify breach - identify how the breach has occurred, for example, whether this is an online attack or data leakage caused accident or intention.
- Investigation and containment - whether internal or external, identify how to restore security considering the breach.
- Impact assessment - once the breach is resolved, a risk assessment will be conducted for individuals and AAUK.
- Recovery - repair the data and systems so that AAUK can continue to operate.
- Notification and communication - establish a communication strategy to inform those individuals affected that a data breach has occurred and report the incident to the Information Commissioner's Office no later than 72 hours after the breach is discovered.
- Evaluation and improvement – all incidents will be fully investigated and evaluated and if necessary changes made to increase security measures.

CONDITIONS OF PROCESSING AND CONSENT

For it to be legal and appropriate for Anderson Accountancy (UK) Ltd to process personal data, at least one of the following conditions must be met:

1. The data subject has given their consent;
2. The processing is required to carry out the functions of a professional accountancy practice in the fulfilment of its contractual obligations agreed with the data subject;
3. It is necessary due to a legal or regulatory obligation;
4. It is necessary to protect someone's vital interests;
5. It is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the AAUK;
6. It is necessary for the legitimate interests of the AAUK or a relevant third party and does not interfere with the rights and freedoms of the data subject.

All processing of personal data carried out by AAUK must meet one or more of the conditions above. Data is only stored to meet the legitimate interests of the AAUK as detailed in Appendix 1 and may be stored securely in any of AAUK's software databases as appropriate to the nature of the engagement with the data subject and on AAUK's secure servers. Hardcopy data is stored in secure filing cabinets and any data considered expired and no longer required for retention under legislation or other statutory requirements is destroyed via secure shredding. The date and method of consent obtained by data subjects is recorded in the data subject's relevant hardcopy file.

TRANSFER OF DATA ELECTRONICALLY

Anderson Accountancy (UK) Ltd utilises technology as much as possible for the quick and efficient transmittance of information to the client and in most cases, this is via electronic mail systems. Where the data being transmitted contains sensitive or personally identifiable information, AAUK will require the data subject to provide a password for the security of the data. AAUK will store this password in

accordance with this policy but accepts no liability or responsibility for the password, its design or storage by 3rd parties including the data subject.

The password will be collected as part of the client take on procedure and the data subject will have the option to change this at any time by contacting the Data Protection Officer at AAUK.

INDIVIDUAL RIGHTS

GDPR gives individuals the right to access personal information held about them by AAUK. The purpose of a "subject access request" is to allow individuals to confirm the accuracy of personal data and check the lawfulness of processing to allow them to exercise rights of correction or objection if necessary. Individuals also have the following rights under GDPR which are applicable:

- **Right to Object** – individuals can object to specific types of processing, including processing for direct marketing.
- **Right to be forgotten (erasure)** – individuals have the right to have their data erased in certain situations such as where the data are no longer required for the purpose for which they were collected; the individual withdraws consent or the information is being processed unlawfully. AAUK may issue an exemption to this if the individual is or has been subject to disciplinary action or other legislative or regulatory obligations take precedence.
- Rights in relation to automated **decision making and profiling**
- **Right to Rectification** – the right to require a controller to rectify inaccuracies in personal data held about them. In some circumstances, if personal data are incomplete, an individual can require the controller to complete the data, or to record a supplementary statement.
- **Right to Portability** – the data subject has the right to request information about them which is provided in a structured, commonly used and machine-readable form so it can be sent to another data controller.

Individuals can request to see any information that AAUK holds about them which includes copies of correspondence referring to them or opinions expressed about them. However, information may be redacted or otherwise removed from a response if it includes:

- Personal information relating to other individuals (unless their permission has been obtained to release it);
- Confidential information relating to AAUK's business practices;
- Intellectual property;

AAUK will respond to all requests for personal information within 30 days. Depending on the complexity of the request, AAUK may charge an administration fee of £10.00 per request. A data request can only be made by the individual that it concerns. Individuals seeking access requests must contact The Data Protection Officer, Anderson Accountancy (UK) Ltd, 33 Taranto Road, Southampton, SO16 5PL, Tel. +44 01794 521300

The following information must be included with the request:

- Full name and date of birth
- Preferred contact details

Along with a full description of the information requested, providing as much information as possible to help AAUK locate the information such as the time periods concerned. It may be necessary for AAUK to seek further clarification if we do not have enough detail to enable us to find the information being sought.

LAW ENFORCEMENT REQUEST AND DISCLOSURE

In accordance with current legislation, AAUK will share an individual's data for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the prevention of financial crime, terrorist financing and anti-money laundering.

DATA RETENTION

Retention periods are set based on legal and regulatory requirements, legitimate business interests, the needs of the individual and good practice guidance. Personal data must only be kept for the length of time necessary to perform the processing for which it was collected. Once information is no longer needed it should be disposed of securely. Paper records should be shredded or disposed of in confidential waste facilities and electronic records should be permanently deleted. If data is fully anonymised then there are no time limits on storage.

AAUK's policy on data retention is to hold information on data subjects for a period of at least 6 years plus the current year.

THIRD PARTIES AND SUPPLIERS

AAUK's long standing policy is never to engage the services of 3rd parties for the deliverance of client services (such as outsourcing bookkeeping services) however, certain conditions need to be met before personal data can be shared with a third party or before an external data processor is used to process data on behalf of AAUK. As a rule, only specific personal data required to fulfil the process will be passed on to third parties and suppliers and must also meet the terms below:

- Any transfers of personal data must meet the data processing principles, it must be lawful and fair to the data subjects concerned.

- It must meet one of the conditions of processing. For example, legitimate reasons for transferring data would include that there is a legal requirement or that it is necessary for the official business of AAUK.

- If no other conditions are met then consent must be obtained from the individuals concerned and appropriate privacy notices provided. That AAUK is satisfied that the third party will meet all the requirements of GDPR particularly in terms of holding the information securely.

- Where a third party is processing personal data on behalf of the AAUK a written contract must be in place.

DIRECT MARKETING

Direct marketing relates to communication (regardless of media) with respect to advertising or marketing material that is directed to individuals; AAUK provides only one form of direct marketing

which would be contained within the newsletter. AAUK provides a clear opt-out provision and individuals are given the opportunity to remove themselves from lists or databases used for direct marketing purposes. AAUK ceases direct marketing activity if an individual requests the marketing to stop.

IMPACT OF NON-COMPLIANCE

All AAUK staff are required to comply with this Data Protection Policy, its supporting guidance and the requirements specified in the GDPR. Any member of staff who is found to have made an unauthorised disclosure of personal information or breached the terms of this Policy may be subject to disciplinary action.

ROLES AND RESPONSIBILITIES

As AAUK processes 'personal data' of clients, staff and other individuals, it is defined as a Data Controller for the purposes of the GDPR. The Data Protection Officer (DPO) is responsible for ensuring AAUK's compliance with the GDPR, for overseeing the data processing and the monitoring, revision and updating of this policy document on an annual basis or sooner, should the need arise.
The Data Protection Officer's responsibilities include:

- ensuring that the policy is produced and kept up to date
- ensuring that the appropriate practice and procedures are adopted and followed by the AAUK
- providing advice and support on data protection issues within the organisation
- working collaboratively with department heads to help set the standard of data protection training for staff
- ensuring compliance with individual rights, including subject access requests
- acting as a central point of contact on data protection issues within the organisation.
- implementing an effective framework for the management of data protection
- ensuring the security measures are effective and the process is regularly tested, assessed and evaluated

In the first instance all enquiries or requests for further information or guidance relating to data protection should be addressed to the Data Protection Officer, Anderson Accountancy (UK) Ltd, 33 Taranto Road, Southampton, SO16 5PL, tel. 01794 521300.

ANDERSON ACCOUNTANCY AS A DATA PROCESSOR

In certain circumstances, AAUK will act as a data processor – particularly in the case of the provision of payroll services. AAUK provides the service to the client who employ data subjects therefore the client becomes the controller and AAUK the processor.

It is required that, in this instance, the client produces their own GDPR policy and notifies their data subjects of this arrangement. Upon request, AAUK will provide to the client an external policy document detailing the information collected about their data subjects, why it is collected and how it is stored.

APPENDICES

Appendix 1

Assessment of Legitimate Interests	How we use your data	Our reasons
AAUK Clients	To deliver services To manage payments To detect, investigate, report, and seek to prevent financial crime. To manage risk To develop and carry out our marketing activities To obey laws and regulations applicable to AAUK To respond to complaints and seek to resolve them	Fulfilling our functions as a recognised professional accounting practice body Our legitimate business interests Our legal duty
AAUK Suppliers	To deliver prompt and accurate processing of supplier invoices To provide prompt and accurate processing of supplier payments	Our legitimate business interests Our legal duty

Appendix 2

Personally identifiable information collected by AAUK consists of the following items:-

Name(s) of the individual
Address
Date of birth
Unique Tax Reference number
National Insurance Number
2 forms of identification including 1 photographic
Telephone number
Email address