Rationale

KellyATC Ltd (KellyATC) is committed to a policy of protecting the rights and privacy of individuals, including clients, staff and others, in accordance with the General Data Protection Regulation (GDPR) May 2018.

The new regulatory environment demands higher transparency and accountability in how companies manage and use personal data. It also accords new and stronger rights for individuals to understand and control that use.

The GDPR contains provisions that the company will need to be aware of as data controllers, including provisions intended to enhance the protection of clients' personal data. For example, the GDPR requires that:

We must ensure that our company privacy notices are written in a clear, plain way that staff and clients will understand.

KellyATC needs to process certain information about its staff, clients and other individuals with whom it has a relationship for various purposes such as, but not limited to:

1. The recruitment and payment of staff.
2. The administration of AML regulations and practice management.
3. Client services – Payroll, Tax Returns, Bookkeeping, Management and Financial Reports.
4. Collecting fees.
5. Complying with legal obligations to Government and Law enforcement.

To comply with various legal obligations, including the obligations imposed on it by the General Data Protection Regulation (GDPR) KellyATC must ensure that all this information about individuals is collected and used fairly, stored safely and securely, and not disclosed to any third party unlawfully.

Compliance

This policy applies to all staff of KELLYATC. Any breach of this policy or of the Regulation itself will be considered an offence and the Company's disciplinary procedures will be invoked.

As a matter of best practice, other agencies and individuals working with KELLYATC and who have access to personal information, will be expected to read and comply with this policy. It is expected that departments who are responsible for dealing with external bodies will take the responsibility for ensuring that such bodies sign a contract which among other things will include an agreement to abide by this policy.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments to the GDPR and other relevant legislation.

The Code of Practice on GDPR for KELLYATC gives further detailed guidance and KELLYATC undertakes to adopt and comply with this Code of Practice.

General Data Protection Regulation (GDPR)

This piece of legislation comes in to force on the 25th May 2018. The GDPR regulates the processing of personal data, and protects the rights and privacy of all living individuals (including children), for example by giving all

individuals who are the subject of personal data a general right of access to the personal data which relates to them. Individuals can exercise the right to gain access to their information by means of a 'subject access request'. Personal data is information relating to an individual and may be in hard or soft copy (paper/manual files; electronic records; photographs; CCTV images), and may include facts or opinions about a person.

For more detailed information on these Regulations see the Data Protection Data Sharing Code of Practice (DPCoP) from the Information Commissioner's Office (ICO). Please follow this link to the ICO's website (www.ico.gov.uk)

Responsibilities under the GDPR

KellyATC will be the 'data controller' under the terms of the legislation – this means it is ultimately responsible for controlling the use and processing of the personal data. The Company appoints a Data Protection Officer (DPO), currently KellyATC who is available to address any concerns regarding the data held by Company and how it is processed, held and used.

Details of the Company's notification can be found on the Office of the Information Commissioner's website. Our data registration number is: ZA068705.

Compliance with the legislation is the personal responsibility of all members of the Company who process personal information.

Individuals who provide personal data to the Company are responsible for ensuring that the information is accurate and up-to-date.

Data Protection Principles

The legislation places a responsibility on every data controller to process any personal data in accordance with the eight principles. More detailed guidance on how to comply with these principles can be found on the ICO's website (www.ico.gov.uk)

In order to comply with its obligations, KellyATC undertakes to adhere to the eight principles:

1) ***Process personal data fairly and lawfully.***
KELLYATC will make all reasonable efforts to ensure that individuals who are the focus of the personal data (data subjects) are informed of the identity of the data controller, the purposes of the processing, any disclosures to third parties that are envisaged; given an indication of the period for which the data will be kept, and any other information which may be relevant.

2) ***Process the data for the specific and lawful purpose for which it collected that data and not further process the data in a manner incompatible with this purpose.***
KELLYATC will ensure that the reason for which it collected the data originally is the only reason for which it processes those data, unless the individual is informed of any additional processing before it takes place.

3) ***Ensure that the data is adequate, relevant and not excessive in relation to the purpose for which it is processed.***
KELLYATC will not seek to collect any personal data which is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will always be drafted with this mind. If any irrelevant data are

given by individuals, they will be destroyed immediately.

4) *Keep personal data accurate and, where necessary, up to date.*

KELLYATC will review and update all data on a regular basis. It is the responsibility of the individuals giving their personal data to ensure that this is accurate, and each individual should notify the Company if, for example, a change in circumstances mean that the data needs to be updated. It is the responsibility of the Company to ensure that any notification regarding the change is noted and acted on.

5) *Only keep personal data for as long as is necessary.*

KELLYATC undertakes not to retain personal data for longer than is necessary to ensure compliance with the legislation, and any other statutory requirements. This means KELLYATC will undertake a regular review of the information held and implement a weeding process.

KELLYATC will dispose of any personal data in a way that protects the rights and privacy of the individual concerned (e.g. secure electronic deletion, shredding and disposal of hard copy files as confidential waste).

6) *Process personal data in accordance with the rights of the data subject under the legislation.*

Individuals have various rights under the legislation including a right to:

- be told the nature of the information the Company holds and any parties to whom this may be disclosed.
- prevent processing likely to cause damage or distress.
- prevent processing for purposes of direct marketing.
- be informed about the mechanics of any automated decision taking process that will significantly affect them.
- not have significant decisions that will affect them taken solely by automated process.
- sue for compensation if they suffer damage by any contravention of the legislation.
- take action to rectify, block, erase or destroy inaccurate data.
- request that the Office of the Information Commissioner assess whether any provision of the Act has been contravened.

KELLYATC will only process personal data in accordance with individuals' rights.

7) *Put appropriate technical and organisational measures in place against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of data.*

All members of staff are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorised third parties. KELLYATC will ensure that all personal data is accessible only to those who have a valid reason for using it.

KELLYATC will have in place appropriate security measures e.g.

- keeping all personal data in a lockable cabinet with key-controlled access.
- password protecting personal data transfered electronically.
- placing any PCs or terminals, CCTV camera screens etc. that show personal data so that they are not visible except to authorised staff.
- ensuring that PC screens are not left unattended without a password protected screen-saver being used.

In addition, KELLYATC will put in place appropriate measures for the deletion of personal data - manual records will be shredded. Hard drives of redundant PCs will be wiped clean before disposal or if that is not possible, destroyed physically. A digital shredder shall be made available for the deletion of personal data on digital files.

This policy also applies to staff who process personal data 'off-site', e.g. when working at home, and in circumstances additional care must be taken regarding the security of the data.

8) ***Ensure that no personal data is transferred to a country or a territory outside the European Economic Area (EEA) unless that country or territory ensures adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.***

KELLYATC will not transfer data to such territories without the explicit consent of the individual.

KellyATC will maintain a risk assessment of the software/web services used and the location of their data storage. Also contained in this assessment shall be the protection measure of the provider.

If the Company collects personal data in any form via its website, it will provide a clear and detailed privacy statement prominently on the website, and wherever else personal data is collected.

Contract as a basis for processing

KELLYATC is required to process personal data on the lawful basis of contract:

- To fulfil our contractual obligations (under the clients engagement letter)
- Because KellyATC have been asked you to do something before entering into a contract (eg provide a quote).

Legal Obligation as a basis for processing

KELLYATC is required to process personal data on the lawful basis of legal obligation:

- To process the personal data to comply with a common law or statutory obligations (eg. AML legislation)

KELLYATC will ensure that any forms used to gather data on an individual will contain a statement explaining the use of that data, and how the data may be disclosed.

Subject Access Rights (SARs)

Individuals have a right to access any personal data relating to them which are held by the Company. Any individual wishing to exercise this right should apply in writing to the Data Controller. Any member of staff receiving a SAR should forward this to the Data Controller.
The Company reserves the right to charge a fee for data subject access requests (currently £20).
Under the terms of the legislation, any such requests must be complied with within 40 days.

For detailed guidance on responding to SARs, see the CoP.

Disclosure of Data

Only disclosures which have been notified under the Company's DP notification must be made and therefore staff should exercise caution when asked to disclose personal data held on another individual or third party.
KELLYATC undertakes not to disclose personal data to unauthorised third parties, including family members, friends, government bodies and in some circumstances, the police.

Legitimate disclosures may occur in the following instances:

- the individual has given their consent to the disclosure.
- the disclosure has been notified to the OIC and is in the legitimate interests of the Company.
- the disclosure is required for the performance of a contract.

There are other instances when the legislation permits disclosure without the consent of the individual.
For detailed guidance on disclosures see the Code of Practice (CoP).

In no circumstances will KELLYATC sell any of its databases to a third party.

Procedure for review

This policy will be updated as necessary to reflect best practice or future amendments made to the General Data Protection Regulation (GDPR) May 2018 and Data Protection Act 1998.

Please follow this link to the ICO's website (www.ico.gov.uk) which provides further detailed guidance on a range of topics including individuals' rights, exemptions from the Act, dealing with subject access requests, how to handle requests from third parties for personal data to be disclosed etc. In particular, you may find it helpful to read the Guide to Data Protection which is available from the website.

For help or advice on any data protection or freedom of information issues, please do not hesitate to contact:

The Data Protection Officer (DPO): Kelly Philpotts, Director.