CPAA - Draft Data Protection Policy

Purpose

This policy has been created to help demonstrate that the Certified Public Accountants Association (CPAA, or, the Association) is compliant with current data protection legislation and to detail various systems and procedures which must be followed by all employees, contractors and relevant officials of the Association.

Policy Statement

The Association takes its responsibilities under data protection legislation extremely seriously. Breach of our data protection responsibilities can result in significant financial and reputational damage. We therefore endeavour to implement practices which ensure that we are constantly upholding our responsibilities under data protection legislation and allow us to meet our users' expectations in terms of privacy.

General Data Protection Regulation

The primary legislation in the United Kingdom governing data protection is the General Data Protection Regulation (GDPR). The legislation covers personal data. Personal data means any information relating to an identifiable person who can be directly or indirectly identified, in particular by reference to an identifier.

The legislation applies to both data controllers and processors. Data controllers determine the purposes and means of processing personal data, while data processors are responsible for processing data on behalf of a controller. The Association is primarily a data controller. The Association does use data processors for certain types of data, in certain circumstances, this does not in any way lessen the Association's obligations.

The five principles, established under this legislation and the Regulation, which organisations must meet, require personal data to be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest shall not be considered to be incompatible with the initial purposes
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data

may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest subject to implementation of the appropriate technical and organisational measures in order to safeguard the rights and freedoms of individuals; and

6. 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

Data Protection Officer

Details of the current data protection officer can be found at the bottom of this policy, under 'Contacting the Association Regarding this Policy' section of this document.

Privacy Notices (Right to be Informed)

When the Association processes personal data for a group of data subjects a privacy notice will be created. Privacy notices contain important information relating to why and how the data is processed. In particular all privacy notices must contain details of; the identity and contact details of the controller and the data protection officer; what data is being collected; why the data is being processed and the lawful basis for the processing; who has access to the data; where the data will be stored; who the data will be transferred to, including details of any third country and applicable safeguards; where the data has been obtained, if the Association has not collected the data directly; how any automated decision has been made; the individual's rights.

As the Association processes information for many different purposes several privacy notices are maintained, which are relevant to different people based upon their relationship/interaction with the Association. It should be noted that it is possible that more than one privacy notice may apply if an individual has or has had multiple different relationships/interactions with the Association.

Relevant privacy notices are provided at the point at which data is collected. If data is not being collected directly then the notice will be provided without delay. All privacy notices are published on the Association's website.

Access Requests (Right of Access)

All individuals have a right to obtain; confirmation that their data is being processed; access to their personal data; and, other supplementary information (which can largely be found in the applicable privacy notice(s)). Any individual wishing to obtain any of these should contact the Association using details provided in the 'Contacting the Association Regarding this Policy' section of this document.

All accesses requests will be completed free of charge, unless the request is manifestly unfounded or excessive. If the request is deemed by the Association to be manifestly unfounded or excessive, the individual will receive a written explanation as to why and details of costs associated with fulfilling the request. The fee charged will be based upon; administration time costs; postage costs; printing costs; and, any other delivery cost.

In exceptional circumstances the Association may refuse an accesses request. An access request will only be refused if it is manifestly unfounded or excessive. If the request is deemed by the Association to be manifestly unfounded or excessive, the individual will receive a written explanation as to why and a statement that the request cannot be processed.

Inaccurate or Incorrect Data (Right to Rectification)

The Association aims to ensure that all data it holds is accurate and correct. However, from time to time, this aim may not be met. All individuals have a right for inaccurate or incorrect data to be corrected or rectified. Any individual wishing to have their data corrected should contact the Association using details provided in the 'Contacting the Association Regarding this Policy' section of this document.

Where data has been transferred to a third party and subsequently it has been rectified, the Association will notify the third party without delay of the rectification.

In some instances, the Association may not take action to a right to rectification request (for example, if it is believed that the request has malicious intent or is inaccurate). If no action is to be taken, a written explanation will be provided to the individual who made the request.

Request to Delete Data (Right to Erasure)

The Association aims to retain data only if it is needed. However, from time to time, this aim may not be met, or a valid reason as to why the data no longer needs to be retained may be presented which had not been considered by the Association. All individuals have a right to request the deletion or removal of personal data where there is no compelling reason for its continued processing. Any individual wishing to have their data erased should contact the Association using details provided in the 'Contacting the Association Regarding this Policy' section of this document.

In limited circumstances the Association will not be able to comply with a request to delete or remove data. This will normally be because the data is being used to; comply with a legal obligation for the performance of a public interest task or in exercising official authority; or, exercise or defend legal claims. If no action is to be taken, a written explanation will be provided to the individual who made the request.

Request to Suppress Processing of Data (Right to Restrict Processing)

Restricting processing means the Association will continue to store the personal data, but will not 'use' the data or transfer it to third parties.

The Association will restrict processing; if you contest the accuracy of the personal data we hold, the restriction will apply until such a time as we have verified the accuracy of the data; if you have objected to the processing and we are considering if we have legitimate grounds not to act on your objection; if the processing we are conducting is found to be unlawful, but you oppose erasure; if we no longer require the data, but you require the data to establish, exercise or defend a legal claim. Any individual wishing to restrict processing of personal data should contact the Association using details provided in the 'Contacting the Association Regarding this Policy' section of this document.

If data has been passed to third parties, the Association will inform them of any restriction to processing as soon as possible.

The Association may have to retain certain personal data, either for a defined period of time or indefinitely, to ensure that a restriction on processing is enforced. This will always be explained in writing to the relevant individual.

Reusing Personal Data (Right to Data Portability)

Personal data can, on the request of the individual, be transmitted to other organisations, or, provided to the individual in a format which they can reuse. All individuals have a right to obtain and reuse their personal data across different services. Any individual wishing to reuse their personal data should contact the Association using details provided in the 'Contacting the Association Regarding this Policy' section of this document.

Before providing data, the Association will take reasonable steps to ensure that the individual making the request has a right to the data they are asking for. This may include providing a copy of government issued ID.

Data provided as part of the right to data portability will always be provided in a structured, commonly used and machine-readable format, normally a CSV file.

The Association welcomes information which members have transferred from another organisation. All reasonable measures will be taken to facilitate the right to data portability.

In some cases, where the request is complex, or we have received several requests, we may require an additional two months to comply with a request to be processed. If this is the case a written explanation will always be provided to the individual concerned within one month of receiving a request.

Objections to Data Processing (Right to Object)

If the Association is processing data based on legitimate interests, for direct marketing or for statistical purposes individuals have the right to object. To object the individual must have grounds relating to your situation.

If the objection relates to the Association using an individual's personal data for direct marketing purposes, then the Association will cease to process the data immediately.

Any objections should be made using the details provided in the 'Contacting the Association Regarding this Policy' section of this document.

Automated Decision Making

The only automated decision-making process operated by the Association is the 'apply online' system, used by those wishing to make an application for membership.

Any individual who has completed the 'apply online' process may challenge the decision made by the system. Any individual wishing to challenge a decision should contact the Association using details provided in the 'Contacting the Association Regarding this Policy' section of this document.

The 'apply online' system is checked regularly to ensure that it is working appropriately. If a fault is found in the system, the live system will be rolled back to an earlier version and the fault rectified.

Special Categories of Data and Data Concerning Criminal Convictions

In carrying out its various functions the Association may collect special categories of data. Specific details of when and why this data is collected can be found in the relevant privacy notice.

The Association treats all personal data it holds and processes carefully, though we always hold ourselves to a higher standard when holding and processing special category data. To this end we always ensure that a privacy impact assessment is conducted for each special category of data we collect.

Contracts

Whenever the Association appoints a processor a written contract must be in place. These contracts are required under data protection legislation. They also help to clarify the purpose of the arrangement and ensure all parties are aware of their responsibilities.

These contacts must include appropriate clauses to ensure; compliance with data protection legislation; appropriate safeguards are in place; and, that each party is aware of their responsibilities and obligations, concerning the protection of the personal data. In particular contracts must contain details of; the subject matter and duration of the processing; the nature and purpose of the processing; the type of personal data; categories of data subject; and, the obligations and rights of the controller.

Copies of all contracts must be retained for the length of the agreement. Once a contract has expired a copy must be retained for six years.

Documentation

The Association produces written records of its processing activities, in addition to privacy notices. These documents may be requested by the Information Commissioner's Office at any time.

The following information must always be documented; the name and contact details of the Association, other controller, representatives and the data protection officer; the purpose of the processing; description of the categories of individuals and categories of personal data; the categories of the recipients of personal data; details of any transfers to third countries, including documenting the transfer mechanism safeguards in place; retention schedules; a description of technical and organisational security measures. Additional information may be documented if it is deemed to be relevant.

Data Protection Impact Assessments

Data protection impact assessments can be used to help the Association meet its data protection obligations and meet individuals' expectations of privacy. They allow the Association to identify and fix problems at an early stage, helping to reduce future costs and reputational damage.

Data protection impact assessments must be carried out; when new technologies are used by the Association; and, if the processing is likely to result in a high risk to the rights and freedoms of individuals.

Response Time

For requests made under this policy and wider data protection legislation we will comply without delay and within one month of receipt of the request, unless otherwise stated in this policy.

If we are unable to meet this commitment for valid reasons allowed under data protection legislation, we will write to explain why, without delay and within one month of receipt of the request.

Security

The Association places significant importance upon the personal data it processes. All personal data should be password protected, and the password only given to those who require access to the data and have been given appropriate training. If additional safeguards are felt necessary, these should be implemented and documented.

From time to time data may need to be processed in an environment where it is not password protected. Additional safeguards should be designed and implemented. These additional safeguards should be documented.

International Transfers

From time to time the Association may transfer personal data it holds outside the European Union and European Economic Area. Where this happens, it will always be brought to the attention of the data subject in the applicable privacy notice.

If personal data is transferred outside the European Union or the European Economic Area, appropriate safeguards will always be developed and implemented. Appropriate safeguards include; relevant clauses being entered into contracts; legally binding agreements; and, compliance with an approved code of conduct approved by a supervisory authority.

Personal Data Breaches

A personal data breach is a security incident that has affected the confidentiality, integrity or availability of personal data held by the Association. This means a breach of security has led to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Personal data breaches must be investigated immediately, and measures implemented to contain the breach. They must be immediately reported to the data protection officer. Initially a decision must be made as to the likelihood and severity of the risk to people's rights and freedoms. The ultimate responsibility for making this decision rests with the data protection officer, but those involved with the breach or those responsible for the affected personal data must make an assessment to inform the data protection officer's decision. If it is likely that there will be a risk, then the data protection officer must notify the Information Commissioner's Office within seventy-two hours of the Association becoming aware of the breach.

Data processors appointed by the Association must report any data breach they experience immediately to the Association's data protection officer. The same procedure as a breach experienced by the Association must be followed.

If the breach poses a high risk to the rights and freedoms of individuals, the data protection officer will arrange for the individuals to be notified of the breach. This will happen without delay. This notification will contain; contact details for the data protection officer; a description of the likely consequences of the breach; and, a description of the measures taken, or proposed, to deal with the personal data breach and including, where appropriate, details of the measures to be taken to mitigate any possible adverse effects. The main reason individuals are contacted is so that they may take steps to protect themselves from the effects of the breach. It should be noted that it may be possible the Association has to notify the Information Commissioner's Office but not the individuals affected by the breach.

Full details of all personal data breaches should be recorded in writing. This documentary evidence should contain; a description of the breach; the risk profile of the breach (including severity and likelihood, in relation to its effects upon individuals' rights and freedoms); details

of any remedial action taken; full details of all decisions made; details of reports made; and, details of all individuals/organisations involved in the breach.

Contacting the Association Regarding this Policy

If you need to contact the Association regarding this policy, please email Lee Haywood, who is the current data protection officer: lhaywood@acpa.org.uk. It will help us to handle your communication if in the subject heading you put 'Data Protection' and provide a brief and concise message.

Alternatively, you can write to the Association using the following address: **CPAA, Unit F, Lostock Office Park, Lynstock Way, Lostock, Bolton, Greater Manchester, BL1 4SG.** It will help us to handle your communication if in the subject heading you put 'Data Protection' and provide a brief and concise message.