



DOCUMENT INFORMATION	
Document Title	PRIVACY POLICY
Document Owner	ASSOCIATION OF CERTIFIED PUBLIC ACCOUNTANTS INTERNATIONAL
Version	1.0
Date	10th MAY 2018



Table of Contents

1.	<i>About us</i>	3
2.	<i>Contact details</i>	3
3.	<i>Changes to the privacy policy and your duty to inform us about changes</i>	3
4.	<i>Definitions</i>	3
5.	<i>Categories of information that we collect</i>	4
6.	<i>How we collect your information</i>	4
7.	<i>Why we collect your information</i>	4
8.	<i>Purposes for which we will use your personal data</i>	4
9.	<i>Change of purpose</i>	5
10.	<i>Cookies, Web beacons and other similar technologies</i>	5
11.	<i>Who else may have access to your information</i>	5
12.	<i>Privacy by design</i>	5
13.	<i>Privacy by default</i>	6
14.	<i>Data Security</i>	6
15.	<i>Retention of your information</i>	6
16.	<i>Your rights</i>	6
17.	<i>Your obligations</i>	7
18.	<i>No fee usually required</i>	7
19.	<i>Time limit to respond</i>	7
20.	<i>Data Controller’s Responsibilities</i>	7
21.	<i>Breach of data Privacy Policy</i>	8
22.	<i>Data breach recording</i>	8
23.	<i>Data breach notification</i>	8
24.	<i>Policy changes</i>	8



1. About us

Welcome to ACPAI'S privacy policy.

We respect your privacy and are committed to protecting your personal data. We are the data controller and responsible for your personal data. We have appointed a data protection officer (“DPO”) who is responsible for overseeing questions in relation to this privacy policy. If you have any questions about this privacy policy, including any requests to exercise your legal rights, please contact the DPO at dpo@thecpaint.com.

2. Contact details

Our full details are:

Full name of entity: Association of Certified Public Accountants International

Name of DPO: Athos Georgiou

Email address: dpo@thecpaint.com

3. Changes to the privacy policy and your duty to inform us about changes

This version was last updated on the May the 10th 2018.

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your relationship with the Association.

4. Definitions

Personal data is information that can be related to an individual. Data is considered personal, if the person it concerns can be identified, directly or indirectly.

Sensitive personal data includes data such as: religion, ideological, political views or activities, health, genetic or biometric information, the racial and ethnic origin, administrative or criminal proceedings and sanctions.

Data subject is a physical person to whom personal data relates.

Data processing is any activity or operation performed on personal data, such as the collection, recording, organisation, structuring, storage, alteration, retrieval, erasure archiving, viewing and destruction of personal data.

Disclosure means making personal data accessible.

Data controller is the legal/physical person who decides the purpose and means of processing personal data.



Data processor is the physical or legal person that processes personal data on behalf of the data controller.

5. Categories of information that we collect

We may collect, use, store and transfer different kinds of personal data about you, which we have grouped together as follows:

- **Identity Data** includes first name, last name, username, title, date of birth and gender.
- **Contact Data** includes delivery address, email address and telephone numbers.
- **Technical Data** includes internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access this website. **CONFIRM**
- **Usage Data** includes information about how you use our website, products and services.

6. How we collect your information

We collect your personal data as a candidate applicant, when you send the relevant application forms for membership.

7. Why we collect your information

We will use your personal data in the following circumstances:

- Where it is necessary for our legitimate interests.
- Where we need to comply with a legal or regulatory obligation.
- For management and administrative purposes.

8. Purposes for which we will use your personal data

We have set out below, a description of all the ways we plan to use your personal data, and which of the legal bases we rely on to do so:

- To register you as a new member,
- To manage payments, fees and charges,
- To deliver relevant website content and news to you,



- **Maintain an official register of members**
- **Communication with you**
- **Basis for the Issue of related certificates required**
- **Provide information to remaining members as to your membership**
- Members networking.

9. Change of purpose

We will only use your personal data for the purposes for which we collected it. If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis, which allows us to do so. Your consent will not be necessary in the following case:

- for compliance with legal obligations of the data controller.

10. Cookies, Web beacons and other similar technologies

Our Website uses “cookie”. We use cookies to distinguish you from other visitors, track your IP address and usage of our site, and to indemnify the name of the website from which you linked to our website.

11. Who else may have access to your information

To best serve you, we may share your personal data with service providers that provide support services. They are contractually restricted from using your information in any manner.

12. Privacy by design

When new data processing systems are introduced, we ensure a high standard of data protection. Particularly, any new systems and processes must comply with the following principles:

- a) Technical and organizational measures must be taken to ensure systematic and secure life cycle management of personal data from collection to processing to deletion,
- b) Data processing systems must be aimed at collecting as few personal data as necessary to fulfil the purpose for which the data was collected,
- c) Data processing systems must be adequately protected from unauthorized access through technical and organizational measures,



- d) Data subjects must be provided with transparent, user-friendly and effective means of control concerning their personal data.

13. Privacy by default

We set up data processing systems in a way that the strictest privacy settings apply automatically.

14. Data Security

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

15. Retention of your information

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

16. Your rights

You have the right to:

- a. Request access to your personal data (commonly known as a “data subject access request”). This enables you to receive a copy of the personal data we hold about you.
- b. Request correction of the personal data that we hold about you or do the changes on your own in your profile.



- c. Request erasure of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it.
- d. Request restriction of processing of your personal data.
- e. Request the transfer of your personal data to you or to a third party.

If you wish to exercise any of the rights set out above, please contact us.

17. Your obligations

It is your responsibility to Keep the data of your personal profile updated. The Association or the DPO initially, upon your registration, enters only the following information applicable then:

- a. Full name (first name, surname, other names)
- b. Full address
- c. Contact information (e-mail address, telephone number provided on your application)
- d. Employer and position
- e. Membership registration number and
- f. User name (**available exclusively to you**)

18. No fee usually required

You will not have to pay a fee to access your personal data (or to exercise any of the other rights).

19. Time limit to respond

We try to respond to all legitimate requests within one month.

20. Data Controller's Responsibilities

The Association is responsible for the lawful processing of personal data and compliance with data protection and data security requirements as set out in this policy or pursuant to applicable law.



21. Breach of data Privacy Policy

The potential penalties and damages resulting from a data protection infringement are serious for both the person committing the violation and for the Association. Any violation of this data privacy policy may result in disciplinary regulatory penalties.

22. Data breach recording

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

The Data Protection Officer systematically documents disclosed breaches and evaluates the reasons for the breaches. Furthermore, the Data Protection Officer initiates further required measures to remedy the situation and to prevent breaches from recurring.

23. Data breach notification

The Association must notify a data breach to the relevant Data Protection Authority within 72 hours after becoming aware of it.

Furthermore, if the personal data breach is likely to result in a high risk to the data subject's rights and freedoms the data subject must be informed without delay.

24. Policy changes

We reserve the right to change this policy, and to apply any changes to information previously collected, as permitted by law. If there are material changes to this policy or our information practices change in the future, we will notify you by posting the policy changes on our website.