The Association Specialists Privacy & Data Policy as @ January 2023

The purpose of this website privacy notice is to inform you about our practices in connection with the collection, use and disclosure of the personal data you make available to us.

Our security measures to protect personal data

We maintain reasonable physical, technical and administrative safeguards to help protect against the unauthorized access, use and disclosure of personal data you voluntarily provide to us and we are committed to safeguarding the privacy of our website visitors and service users.

It should be noted that we cannot be held responsible for any personal data you share or post on public spaces, such as our blogs. Such public spaces may be consulted or viewed by anyone visiting our Website and, as such, falls outside the scope of this Policy.

This policy applies where we are acting as a data controller with respect to the personal data of our website visitors and service users; where we determine the purposes and means of the processing of that personal data.

We use cookies on our website to collect anonymous data that helps us improve your web experience. Our website incorporates privacy controls which affect how we will process your personal data. By using the privacy controls, you can specify whether you would like to receive direct marketing communications and limit the publication of your information. You can access the privacy controls via options provided when you visit our sites.

In this policy, "we", "us" and "our" refer to conferences, congresses and events and memberships managed in whole, or in part by *The Association Specialists.*

1. How we use your personal data

- In Section 2 we have set out:
- the general categories of personal data that we may process;
- in the case of personal data that we did not obtain directly from you, the source and specific categories of that data;
- the purposes for which we may process personal data; and
- the legal bases of the processing.
    - We may process data about your use of our website and services ("**usage data**"). The usage data may include your IP address, geographical location, browser type and version, operating system, referral source, length of visit, page views and website navigation paths, as well as information about the timing, frequency and pattern of your service use. The source of the usage data is Google Analytics. This usage data may be processed for the purposes of analysing the use of the website and services. The legal basis for this processing is our legitimate interests, namely monitoring and improving our website and services.
    - We may process information that you provide to us for the purpose of subscribing to our email notifications and/or newsletters ("**notification data**"). The notification data may be processed for the purposes of sending you the relevant notifications and/or newsletters. The legal basis for this processing is your provision of your data and thus your consent.

2. Providing your personal data to others

- We may disclose your personal data to any of our related companies (this means companies with substantially the same shareholding) insofar as reasonably necessary for the purposes, and on the legal bases, set out in this policy.
- We may disclose your personal data to our insurers and/or professional advisers insofar as reasonably necessary for the purposes of obtaining or maintaining insurance coverage, managing risks, obtaining professional advice, or the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure.
- We may disclose your personal data to our suppliers or subcontractors insofar as reasonably necessary to provide information or services requested by you.
- Financial transactions relating to our services may be handled by our payment services providers, SecurePay, a division of Australia Post. We will share transaction data with our payment services providers only to the extent necessary for the purposes of processing your payments, refunding such payments and dealing with complaints and queries relating to such payments and refunds. You can find information about the payment services providers' privacy policies and practices at https://auspost.com.au/privacy
- In addition to the specific disclosures of personal data set out in Section 3, we may disclose your personal data where such disclosure is necessary for compliance with a legal obligation to which we are subject, or in order to protect your vital interests or the vital interests of another natural person. We may also disclose your personal data where such disclosure is necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure.

3. Retaining and deleting personal data

- This Section sets out our data retention policies and procedure, which are designed to help ensure that we comply with our legal obligations in relation to the retention and deletion of personal data.
- Personal data that we process for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- We will retain your personal data as follows:
- Personal data will be retained for a minimum period of twelve (12) months and for a maximum period of three (3) years following your provision of the data / receipt of communication.
    - Notwithstanding the other provisions of this Section, we may retain your personal data where such retention is necessary for compliance with a legal obligation to which we are subject, or in order to protect your vital interests or the vital interests of another natural person.

4. Amendments

- We may update this policy from time to time by publishing a new version on our website.
- You should check this page occasionally to ensure you are happy with any changes to this policy.
- We may notify you of significant changes to this policy by email or through the private messaging system on our website.

5. Your rights under the APP

- In this Section 5, we have summarised the rights that you have under the Australian Privacy Principles (APP) (1988). Some of the rights are complex thus not all of the details have been included in our summaries. Accordingly, you should read the relevant laws and guidance from the regulatory authorities for a full explanation of these rights.
- Your principal rights under the Australian Privacy Principles (APP) (1988) are:

- APP 1 — Open and transparent management of personal information
- APP 2 — Anonymity and pseudonymity
- APP 3 — Collection of solicited personal information
- APP 4 — Dealing with unsolicited personal information
- APP 5 — Notification of the collection of personal information
- APP 6 — Use or disclosure of personal information
- APP 7 — Direct marketing
- APP 8 — Cross-border disclosure of personal information
- APP 9 — Adoption, use or disclosure of government related identifiers
- APP 10 — Quality of personal information
- APP 11 — Security of personal information
- APP 12 — Access to personal information
- APP 13 — Correction of personal information

- You have the right to transparency of how we use your personal information, this includes access to the information held about you, and a clear statement of how this data is being used
- You have the right to request anonymity and/or the use of a pseudonym, subject to certain limitations as defined by the APP
- You have the right to opt-in or out of the collection of your personal data by us or third parties. This data can include information directly relevant to the operation and organisation of events and services, as well as for marketing purposes. When providing consent, you will be provided options to allow you to choose the services and level of consent you prefer.
- We will undertake to handle unsolicited personal information in accordance with APP guidelines and ensure that it is correctly disposed of or otherwise dealt with.
- We will not include personal information in direct marketing campaigns without first seeking and obtaining express consent.
- In the event that your personal data needs to be communicated to an overseas third party, we will undertake to ensure that this party has taken steps to ensure that your privacy is not breached by them under the APP.
- If applicable, we will not adopt, use or disclose any government related identifier unless an exception under the APP applies.
- We will take all reasonable steps to ensure that any data collected is accurate and up-to-date.
- We will undertake to manage a high level of security surrounding the processes of collection and storage of your personal information. This includes the use of technological security measures, as well as internal procedures and training.
- At any time, you will be able to request a report containing all personal information currently stored. This will be provided in an accessible format and delivered in a reasonable timeframe, taking into consideration the volume and complexity of the data retained.
- At any time, you will be able to file for an amendment to your information. We will aim to undertake the requested changes in a reasonable timeframe and provide confirmation of any changes made.
- All reasonable attempts will be made to ensure that data breaches do not occur. However, in the unlikely event of a data breach, we will undertake to inform you and the relevant authorities as soon as possible after receiving notification of the breach.

6. Your rights under GDPR

- In this Section 7, we have summarised the rights that EU Residents have under the General Data Protection Regulation (GDPR) (2018). Some of the rights are complex, and not all of the details have been included in our summaries. Accordingly, you should read the relevant laws and guidance from the regulatory authorities for a full explanation of these rights.
- EU Residents principal rights under the General Data Protection Regulation (GDPR) (2018) are:

    - the right to access;
    - the right to rectification;
    - the right to erasure;
    - the right to restrict processing;
    - the right to object to processing;
    - the right to data portability;
    - the right to complain to a supervisory authority; and
    - the right to withdraw consent.
- You have the right to confirmation as to whether or not we process your personal data and, where we do, access to the personal data, together with certain additional information. That additional information includes details of the purposes of the processing, the categories of personal data concerned and the recipients of the personal data.
- You have the right to have any inaccurate personal data about you rectified and, taking into account the purposes of the processing, to have any incomplete personal data about you completed.
- In some circumstances you have the right to the erasure of your personal data without undue delay. Those circumstances include: the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; you withdraw consent to consent-based processing; you object to the processing under certain rules of applicable data protection law; the processing is for direct marketing purposes; and the personal data have been unlawfully processed. However, there are exclusions of the right to erasure. The general exclusions include where processing is necessary: for exercising the right of freedom of expression and information; for compliance with a legal obligation; or for the establishment, exercise or defence of legal claims.
- In some circumstances you have the right to restrict the processing of your personal data. Those circumstances are: you contest the accuracy of the personal data; processing is unlawful but you oppose erasure; we no longer need the personal data for the purposes of our processing, but you require personal data for the establishment, exercise or defence of legal claims; and you have objected to processing, pending the verification of that objection. Where processing has been restricted on this basis, we may continue to store your personal data. However, we will only otherwise process it: with your consent; for the establishment, exercise or defence of legal claims; for the protection of the rights of another natural or legal person; or for reasons of important public interest.
- You have the right to object to our processing of your personal data on grounds relating to your particular situation, but only to the extent that the legal basis for the processing is that the processing is necessary for: the performance of a task carried out in the public interest or in the exercise of any official authority vested in us; or the purposes of the legitimate interests pursued by us or by a third party. If you make such an objection, we will cease to process the personal information unless we can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms, or the processing is for the establishment, exercise or defence of legal claims.
- You have the right to object to our processing of your personal data for direct marketing purposes (including profiling for direct marketing purposes). If you make such an objection, we will cease to process your personal data for this purpose.
- You have the right to object to our processing of your personal data for scientific or historical research purposes or statistical purposes on grounds relating to your particular situation, unless the processing is necessary for the performance of a task carried out for reasons of public interest.
- To the extent that the legal basis for our processing of your personal data is:
    - consent; or

- that the processing is necessary for the performance of a contract to which you are party or in order to take steps at your request prior to entering into a contract,
- and such processing is carried out by automated means, you have the right to receive your personal data from us in a structured, commonly used and machine-readable format. However, this right does not apply where it would adversely affect the rights and freedoms of others.

- If you consider that our processing of your personal information infringes data protection laws, you have a legal right to lodge a complaint with a supervisory authority responsible for data protection. You may do so in the EU member state of your habitual residence, your place of work or the place of the alleged infringement.
- To the extent that the legal basis for our processing of your personal information is consent, you have the right to withdraw that consent at any time. Withdrawal will not affect the lawfulness of processing before the withdrawal.
- You may exercise any of your rights in relation to your personal data by written notice to us or by email.

7. About cookies

- A cookie is a file containing an identifier (a string of letters and numbers) that is sent by a web server to a web browser and is stored by the browser. The identifier is then sent back to the server each time the browser requests a page from the server.
- Cookies may be either “persistent” cookies or “session” cookies: a persistent cookie will be stored by a web browser and will remain valid until its set expiry date, unless deleted by the user before the expiry date; a session cookie, on the other hand, will expire at the end of the user session, when the web browser is closed.
- Cookies do not typically contain any information that personally identifies a user, but personal information that we store about you may be linked to the information stored in and obtained from cookies.

8. Cookies that we use

- We use cookies for the following purposes:
- authentication – we use cookies to identify you when you visit our website and as you navigate our website
- analysis – we use cookies to help us to analyse the use and performance of our website and services
- cookie consent – we use cookies to store your preferences in relation to the use of cookies more generally

9. Cookies used by our service providers

- Our service providers use cookies and those cookies may be stored on your computer when you visit our website.
- We use Google Analytics to analyse the use of our website. Google Analytics gathers information about website use by means of cookies. The information gathered relating to our website is used to create reports about the use of our website. Google’s privacy policy is available at: https://www.google.com/policies/privacy/.

10. Managing cookies

- Most browsers allow you to refuse to accept cookies and to delete cookies. The methods for doing so vary from browser to browser and from version to version. You can however obtain up-to-date information about blocking and deleting cookies via these links:

- https://support.google.com/chrome/answer/95647?hl=en (Chrome);
- https://support.mozilla.org/en-US/kb/enable-and-disable-cookies-website-preferences (Firefox);
- http://www.opera.com/help/tutorials/security/cookies/ (Opera);
- https://support.microsoft.com/en-gb/help/17442/windows-internet-explorer-delete-manage-cookies (Internet Explorer);
- https://support.apple.com/kb/PH21411 (Safari); and
- https://privacy.microsoft.com/en-us/windows-10-microsoft-edge-and-privacy (Edge).
    - Blocking all cookies will have a negative impact upon the usability of many websites.

11. Data and personal information security

As IT systems and software have evolved over the past few years with most systems now "cloud based", the need for internal IT support within companies has moved to an external support service that ensures your data is secure, there is a well-documented and planned disaster recovery process, and the support is swift to respond. The Association Specialists is no exception to this and as an organisation with responsibility for your and many other clients' data and delegate / member information we take this extremely seriously. We have worked hard with our IT support providers (Portable Systems) based in NSW to put in place rigid controls that comply with the Australian Signals Directorate Small Business Cyber Security Guide (see link below)
https://www.cyber.gov.au/sites/default/files/2021-02/ACSC%20Small%20Business%20Cyber%20Security%20Guide.pdf

In particular, we have made sure your information will be protected in the following ways:

1. Compliance - all software is fully licenced and upgraded with all new releases.
2. Security – we deal with the issues outlined in the Small Business Cyber Security Guide with the following:
    a. Protection against Malicious software, scam emails and ransomware – All staff computers and infrastructure are kept up to date with the latest security and software patches. All client data is backed up to a secure off-site location. We run an advanced email filter and internal training on how to recognise phishing emails. We run an advanced anti-virus application on all staff computers.
    b. The company network is protected by an advanced firewall which also provides secure remote access to staff computers.
    c. We have implemented a secure password sharing system that will protect the logins to the corporate IT accounts that we manage.
    d. We practice the principle of least privilege on our key IT systems. Staff have access only to the functions that they need to do their job.
    e. All staff are required to perform a cyber security training course to ensure that they are aware of the potential risks, how to avoid them and how to report issues that they see.
3. Disaster Recovery – we have a disaster recovery and a business continuity plan to ensure that we are able to respond to major events in a timely and coherent way.
4. IT Support – we engage the services of Portable Systems who are available 24x7 to assist with any major outages.
5. Privacy – TAS staff have contracts of employment which clearly state their requirement to maintain privacy over client information at all times (both during and post-employment). In

addition, the company are aware of the relevant reporting requirements in relation to data breaches and will respond accordingly should this occur.

6. Cyber Insurance – whilst TAS believes it has systems in place which minimise the risk of data breaches, no system is infallible. As a result, TAS has comprehensive Cyber Insurance cover to support us, and your organisation should the need arise.

11. Data protection officer

- The Association Specialists has an appointed data protection officer and they can be contacted via email at privacy@theassociationspecialists.com.au

12. Access, review & correction

- You have the right to access your personal data. For legitimate purposes, you can rectify or oppose to the processing of your personal data. You also are entitled to ask to receive your personal data in a structured and standard format. In case of any such request or complaint, please send an email to privacy@theassociationspecialists.com.au

Our details

The Association Specialists Pty Ltd
You can contact us: by post, to Suite 5.02, Level 5, 655 Pacific Highway, St Leonards, 2065, by email at info@theassociationspecialists.com.au or by telephone, on +61 2 9431 8600