Privacy Policy

This privacy notice discloses the privacy practices of JTA Health, Safety and Noise Specialists solely in relation to our collection of information through our website located at www.jta.com.au.

Information Collection, Use, and Sharing

We are the sole owners of the information collected on this site. We only have access to and can only collect information that you voluntarily give us via email or other direct contact from you. We will not sell or rent this information to anyone.

We will use your information to verify your authority to access any data or reports we have been contracted to prepare for you or the report owner. We will not share your information with any third party or anyone outside of our organisation, other than the report owner to verify your authority to access the data or reports, or unless we are required to do so by law.

If you wish to review any personal information we hold on you, you may request this from us. You may also request to have any of this information rectified, blocked or erased, but in doing so this may alter or restrict your access to our services.

We may contact you via email in the future to share Occupational Health and Safety News, new services, or where we make any material changes to this privacy policy.

Opt Out

You may opt out of any future contacts from us at any time by emailing or calling us. Our contact details are available on our website.

Security

At JTA we take security of information seriously and therefore take extra precautions to protect your information. JTA's virtual servers and data are stored in a purpose built data facility that is secured with biometric fingerprint technology, ID access cards, CCTV and 24/7 onsite security staff. There is an encrypted IPsec VPN connection between JTA's Head Office and the datacentre. Any external users connect via PPTP VPN. Password policies with complexity requirements are configured. Any sensitive documents we provide by email are password protected.

Only employees who need the information to perform a specific job (for example, providing access codes and passwords or customer service) are granted access to personally identifiable information. Any computers or servers in which we store personally identifiable information are kept in a secure environment.

Last Updated 9th August, 2018