



ARKADIA

PRIVACY POLICY 2024

APPROACH TO PRIVACY

Arkadia is committed to protecting the privacy of its employees, clients, customers, suppliers, contractors, and consultants. Arkadia handles personal information in a serious manner, in order to meet the privacy obligations that apply to it under the Privacy Act 1988 (Cth) ('the Privacy Act').

Arkadia collects personal information in order to conduct its business and comply with a range of legislative requirements. The purpose of this policy is to explain how Arkadia handles the collection and use of personal information of those who work with and for Arkadia, for job applicants, for clients, customers, suppliers, contractors, and consultants (hereinafter referred to as "your" or "you"). Arkadia endeavours to ensure that your personal information is used responsibly, ethically and in a transparent manner.

PERSONAL INFORMATION

Personal information is information relating to you which personally identifies you or makes your identity reasonably apparent. By your 'personal information' we mean any information about you, which is reasonably identifiable, that we may collect or use regarding you, as a client or customer, prospective client or customer, member of the public, tenant, third party or employee of a third party we deal with, director, officer or representative. This can include information such as contact information, marketing preferences, identity documents, financial data, complaints and customer inquiries or your use of our website, depending on your interactions with us.

Personal information may also include 'sensitive information'. Sensitive information is information or an opinion about an individual's racial or ethnic origin, political or religious beliefs, membership of a trade or professional association or union, sexual preferences, criminal record, health and biometric information or similar such information. Arkadia will only collect sensitive information if it is necessary for business purposes and will only collect sensitive information with your consent (unless otherwise permitted or required by law).

All information collected will be used and disclosed by Arkadia only in accordance with this policy and the law. Arkadia will take reasonable steps to ensure that all personal information is held securely.



COLLECTION OF PERSONAL INFORMATION ACROSS ARKADIA

Arkadia will only collect personal information from individuals if it is reasonably necessary for the Company's functions or activities.

Arkadia may collect personal identification information from users of our website in a variety of ways, including, but not limited to, when users visit our site, register on the site, place an order, subscribe to the newsletter, fill out a form, and in connection with other activities, services, features or resources we make available on our website. Users may be asked for, as appropriate, name, email address, mailing address, phone number. Users may, however, visit our website anonymously. Arkadia will collect personal identification information from users only if they voluntarily submit such information to us. Users can always refuse to supply personal identification information, except that it may prevent them from engaging in certain website related activities.

Our website may use "cookies" to enhance the user's experience. Web browser places cookies on a user's hard drive for record-keeping purposes and sometimes to track information about them. A user may choose to set their web browser to refuse cookies, or to alert them when cookies are being sent. If they do so, note that some parts of the website may not function properly.

Other general types of personal information collected include:

- Lease arrangements: Arkadia uses personal information for purposes including evaluating whether to grant leases and/ or enter into agreements with prospective tenants, documenting these leases and/or agreements, performing its obligations under leases and/or agreements with tenants, managing relationships with tenants and monitoring properties;
- Hotel guests: Arkadia collects personal information from hotel guests and occupiers (before, during and after their stay, which may include website use, guest survey responses, occupation dates, member services);
- Service providers: we may collect personal information if you work for a company that supplies goods or services to us, particularly relating to financial capacity to perform the services.
- CCTV: images may be collected through CCTV for property security and safety;



- Event photography/videography: imagery from events of special experiences/competitions may be collected and used in marketing/promotional material.

INFORMATION PROVIDED BY AN INDIVIDUAL FOR EMPLOYMENT PURPOSES

It is expected that Arkadia will need to collect personal information from those who work with and for Arkadia. In addition, as part of the recruitment process, Arkadia may obtain information directly from a candidate as a result of their application to a job advertisement.

Furthermore, if a candidate's application is successful, as a condition of employment with Arkadia, the successful candidate will likely be asked to provide evidence of their identity and legal entitlement to work in Australia. It is likely a successful candidate will also be asked to provide personal information, such as emergency contact details, date of birth, tax file number, superannuation and bank account and tax status details, which will form part of an employee file.

Specifically, Arkadia may collect other personal information directly from an individual including:

- Employment applications: information related to your application if you apply for a job with us;
- recruitment and on-boarding information such as an application form and resume, and details of previous employment;
- contact details, including address, email address and phone number;
- details of next of kin and emergency contact details;
- identification documents including passport and drivers' licence;
- marital status and family details, including in relation to personal leave;
- details of share and option plans;
- Know your customer (KYC) checks or anti-money laundering related checks;

INFORMATION PROVIDED BY A THIRD-PARTY

As part of the recruitment process, where relevant, and with the candidate's prior consent, Arkadia may seek information about a candidate through a third-party such as a recruitment service provider or a former employer. With the candidate's consent, Arkadia may also seek information regarding:



- prior employment history through reference checks;
- eligibility to work in Australia through a visa status check;
- educational qualifications by requesting confirmation of qualifications or results from an academic institution;
- interview records and details of any pre-employment assessments, including aptitude or other psychometric testing; and
- a criminal history check.

Arkadia may also access personal information through publicly available professional networking sites such as LinkedIn.

USE OF PERSONAL INFORMATION

The purposes for which Arkadia may collect, use, and disclose personal information include (but are not limited to):

- **Products and services:** to assess, maintain, administer, and provide you with the products or services you have applied for, this may include marketing and analytics: to send you direct marketing communications and information about our services, mostly by email. We may also use your personal information to analyse usage of the program, improve our product, service and membership content and product offers, and conduct advertising and promotions. You have a right to opt-out of receiving any direct marketing communications from us.
- **Memberships:** to provide you with access to our memberships, including discounts, rewards, and members services through the program;
- to assess or respond to claims, complaints, or conduct, or co-operate with investigations when required;
- **Managing shopping centres and other properties:** to provide access to our Wi-Fi services, which may involve collecting information including your device ID, device type, geo-location information on any movement of your device throughout our premises, to facilitate the purchasing, and redemption of shopping centre gift cards, and any other purposes that are incidental to, or directly connected with, the operation of properties;
- **Confirming and verifying your identity:** (this may involve the use of a credit reference agency or other third parties acting as our agents) and to conduct due diligence, including 'Know Your Customer' checks and other procedures that we undertake prior to you becoming our customer. We may also screen against publicly available government and/or law enforcement agency sanctions lists;
- To comply with laws that apply to the product or service you have with us, including anti-money laundering and counter-terrorism financing laws, modern slavery laws, taxation laws and the Foreign Account Tax Compliance Act (FATCA) or Common Reporting Standards (CRS) and



respond to any regulator or legal enforcement investigations or enquiries;

- to run a promotion, contest, survey or other website feature;
- to send periodic emails (whether in response to an order, or otherwise where a customer opts-in to a mailing list. If at any time the User would like to unsubscribe from receiving future emails, we include detailed unsubscribe instructions at the bottom of each email.
- to allow you access to Arkadia's buildings, and to ensure the security of Arkadia buildings, confidential information and other company property;
- to monitor and protect workplace health and safety for individuals working at or visiting our properties. This includes collecting and using CCTV footage;
- to liaise with any insurers in respect of any insurance policies that relate to you or our assets;
- The detection, investigation and prevention of fraud and other crimes or malpractice: for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings), for obtaining legal advice or for establishing, exercising, or defending legal rights;
- Effecting a transaction where a third party is taking control or ownership of a relevant business activity;
- otherwise as permitted or required by law; or
- otherwise with your consent.

ACCURACY AND STORAGE OF PERSONAL INFORMATION

Arkadia will always endeavour to maintain an accurate record of all personal information it holds. Where relevant, individuals should ensure that all personal information provided to Arkadia is accurate and up to date and notify Arkadia of any changes where required.

In addition, in order to ensure personal information is handled appropriately, we require individuals to:

- only access personal data if they need to do so for the proper performance of their role;
- not share personal data unless this is necessary for the proper performance of their role;
- keep personal data secure and protected;
- regularly review and update personal data as necessary;
- not make unnecessary copies of personal data and keep and dispose of any copies securely;
- consider using strong passwords and when protecting documents with personal data on them;



- never leave computers, devices, electronic storage systems, files, paperwork or other things containing personal data in a manner that risks there unauthorised access or theft;
- where appropriate, ensure that highly sensitive personal data is encrypted before being transferred electronically to authorised external contacts. Where necessary, please speak to your manager or the IT department for more information on how to do this;
- where applicable, anonymise data or using separate keys/codes so that the data subject cannot be identified;
- not save personal data to personal computers or other devices;
- not take personal data away from Arkadia's premises unless required to do so for the proper performance of their role;
- shred and/or securely dispose of personal data when finished with; and
- immediately report any loss, unauthorised access, security risk or other issue that arises in respect of personal information to your manager.

Arkadia adopts appropriate data collection, storage and processing practices and security measures to protect against unauthorised access, alteration, disclosure or destruction of your personal information, username, password, transaction information and data stored on its software, hardware, and websites. Arkadia will take reasonable steps to protect your personal information from misuse, interference and loss, unauthorised access, modification or disclosure. We use technologies and processes such as access control procedures, network firewalls, encryption, password protected databases and physical security measures to protect your personal information.

We keep your personal information for only as long as is necessary for the purpose for which we collected it. We will also take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for the purposes stated under this policy.

Sensitive and private data exchange between any Arkadia website and its users happens over an SSL secured communication channel and is encrypted and protected with digital signatures. The Arkadia website has also been designed in compliance with PCI vulnerability standards in order to create as secure of an environment as possible for users.

Importantly, Arkadia does not sell, trade, or rent your personal identification information to others. Arkadia may share generic aggregated demographic information not linked to any personal identification information regarding



visitors and users with Arkadia’s business partners, trusted affiliates and advertisers for the limited purposes outlined in this policy.

ACCESS TO PERSONAL INFORMATION

Personal information held by Arkadia in respect of employees is subject to the “employee records exemption” under the Privacy Act and does not have to be disclosed on request.

Other persons, such as job applicants can request copies of their personal information by contacting the Chief Executive Officer, Arkadia. If personal information is incorrect, individuals may request that Arkadia amend its records and Arkadia will take reasonable steps to do so.

DATA BREACH NOTIFICATION

We will report certain data breaches (known as Notifiable Data Breaches) to you, if you are at likely risk of serious harm, and to the Office of the Australian Information Commissioner as required.

A notifiable data breach may occur where personal information held by us is lost or subjected to unauthorised access or unauthorised disclosure.

RAISING A CONCERN OR A COMPLAINT

If you have questions about how Arkadia handles your personal information, or if you have a complaint about Arkadia’s information handling practices, you can contact Arkadia’s General Counsel as follows:

Email: dkhoury@arkadia.com.au

Phone: (02) 9908 0355

Mail: Level 1, 201 Military Rd, Neutral Bay NSW 2089

Arkadia will endeavour to provide a reply to your written request within 21 days. If you are not satisfied with the decision, you can contact us to discuss your concerns. If the complaint remains unresolved, you have the option of notifying the Office of the Australian Information Commission.



This policy will be reviewed if there are changes to the legal or regulatory framework which applies to this policy. We will notify any changes by posting an updated version of this policy on this website.