HPA

PRIVACY POLICY

Contents

1. Purpose

The purpose of this policy is to explain how Hop Products Australia ("HPA") handles personal information of employees, contractors, job applicants, suppliers, and customers.

2. Scope

This policy applies to all persons who deal with HPA.

3. Introduction

Hop Products Australia will be referred to as "HPA", "we", "our", or "us" in this policy.

HPA is committed to protecting the privacy of its employees and meeting any privacy obligations set out in the Privacy Act 1988 (Cth) ("the Act") and Australian data protection laws. We make every effort to maintain the highest standards in dealing with the personal information of all people that we deal with (including employees and people external to the organisation referred to in this document as "you" or "your") in accordance with the Act.

This Privacy Policy sets out how HPA collects, uses, discloses, manages, and protects personal information about you. It also explains how to contact us if you have any questions about the management of your personal information or would like to access the personal information we hold about you.

HPA may unilaterally introduce, vary, or replace this policy at any time from time to time.

4. The information we collect and hold

We may collect and hold personal information about you if it is reasonably necessary for HPA's functions or activities. This may contain information that can identify you, and is relevant to liaising with you, or to providing funding or services to you or others.

4.1 Information provided by an individual

It is HPA's usual practice to collect personal information from those who work with and for HPA. In addition, as part of the recruitment process, HPA may obtain information directly from a candidate as a result of their application to a job advertisement.

If a candidate's application is successful, as a condition of employment with HPA, the candidate will likely be asked to provide evidence of their identity and legal entitlement to work in Australia. The successful candidate will also be asked to provide personal information which will form part of an employee file.

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

- Recruitment and onboarding information such as cover letter, resume, qualifications, and details of previous employment;
- Contact details, including address, email address, and phone number;
- Date of birth;

- Details of next of kin and emergency contact details;
- Gender;
- Nationality;
- Identification documents including passport and drivers' licence;
- Marital status and family details, including in relation to personal leave;
- Bank account details (including bank name and location, BSB, and account number); and
- Tax file number and information in relation to tax status.

4.2 Information provided by a third-party

As part of the recruitment process, where relevant, and with the candidate's consent, HPA 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, HPA 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 psychometric testing; and
- Ability to perform the inherent requirements of the role, through medical and other allied health professionals, or criminal history check and/or working with children check.

HPA may also access personal information through publicly available networking sites such as Facebook or LinkedIn.

4.3 Information collected during employment

HPA may collect information about an individual and their work throughout their employment with HPA, (or for contractors during the performance of a contract with HPA). Such information may include:

- Details of any contract of employment (or contract for services) including start and end dates, department, role and location, reporting lines, title (including details of previous titles), working days and hours, details of promotions, details of bonuses, remuneration and salary (including details of previous remuneration), benefits and entitlements;
- Any information relating to disciplinary or grievance investigations and proceedings, including any warnings and related correspondence;
- Information relating to performance and behaviour at work, including appraisals, ratings, performance reviews, objectives, goals, and performance improvement plans;
- Details of attendance at work and absences, including annual and personal leave;
- Training records including training needs;
- Details of any expenses claimed; and
- Details of the use of HPA property and equipment (including computers, swipe cards, and telephone systems), emails, and software.

HPA may also collect other personal information if required or authorised to do so by law.

4.4 Information collected about supplier and customers

It is usual practice for HPA to collect personal information about its suppliers and customers to facilitate the normal course of business operations. Such information may include:

- Business name and address;
- Contact details;
- Key employee names.

We only collect Sensitive Information (as defined by the Act) in very specific circumstances. Where we do so, we will notify you of this and ask for your specific consent for its collection, use, and disclosure with strict controls around this.

4.5 Collection of information that is not personal information

We also collect information about your interaction with our website, activities, and events without identifying you as an individual. Please refer to Clause 13 below for further details.

5. How we collect and hold information

Personal information will generally be collected directly from you using any of our standard forms, in a customer or supplier contract, over the internet, via our website, email, or through a telephone conversation with you.

6. Use of personal information

The personal information that we collect and hold about you, depends on your interaction with us. Generally, we will collect, use and hold your personal information for the purposes of:

a) Providing products to you or someone else;

b) Providing you with information about other products that we, our related entities and other organisations that we have affiliations with, offer that may be of interest to you;

c) Facilitating our internal business operations (including managing your employment, if relevant);

d) Complying with regulatory or legal requirements;

e) Analysing our goods and customer needs with a view to developing new or improved services

7. What we do with the information we collect

HPA does not sell or otherwise trade your personal information. Generally, we only use or disclose personal information about you for the purposes for which it was collected (as above).

We use your personal information to carry out our interaction with you, including understanding your needs and providing better products. In particular, we use your personal information, and you

consent to us using your personal information:

- For internal record keeping and work-related administrative purposes;
- To establish, maintain and manage relationships, including to serve functions such as recruitment, payroll, reimbursements, appraisals, and any disciplinary action (including any termination of any employment or engagement) and managing employees' work and any claim concerning any injuries or illnesses;
- To run HPA business operations and support future planning;
- To improve our products;
- For promotion and direct marketing to you of our products;
- For internal product/service analysis (market research);
- To comply with all applicable laws and protect against fraudulent activity;
- To conduct market research and analysis to improve our offering;
- To conduct competitions or promotions for us;
- To verify your identity, including confirming work eligibility;
- To investigate any complaints made by you, or against you;
- If we have reason to suspect that you have been engaged in any unlawful activity; or
- Otherwise with your consent.

We also use your personal information to communicate with you, including by email, mail, or telephone. If you have opted in to receive newsletters, communications, or special offers from HPA you may, in some circumstances, also receive newsletters, communications, or special offers from third-party partners.

8. When we disclose your personal information

We may disclose personal information held about you to:

a) Our related companies as required for carrying on our business;

b) Third party service suppliers, including, but not limited to email systems providers and parties involved in the maintenance of our information technology systems;

c) Our authorised representatives (including banking, accounting, legal and financial advisers);

d) Organisations required by law;

e) Travel agents and suppliers of accommodation and travel services;

f) Insurance providers about specific claims;

g) Government agencies such as ATO, Fair Work Ombudsman, Workcover, etc.

h) Superannuation funds;

i) Law enforcement agencies; and,

j) To other third parties as allowed by law or with your consent.

9. Security

HPA complies with Australian data protection laws. We are committed to ensuring that your information is secure. To prevent unauthorised access, disclosure, misuse, modification, or loss of your personal information, we have in place suitable physical, electronic, and managerial procedures to safeguard and secure the information.

Access to your personal information is limited to those parties within HPA who require legitimate access to it.

Because some of our back-ups are cloud-based, your information may also be stored on computer servers located outside of Australia, in particular, Hong Kong, Japan, Malaysia, Singapore, and Korea. You consent to the disclosure of your personal information to such overseas recipients and its location on overseas servers.

In special circumstances – for example, if we were to sell our business or part of it, your information may be transferred to third parties and their advisers as part of that sale. From time to time, we may provide aggregated and de-identified information to other organisation partners for various purposes.

If you receive communications purporting to be connected with us or our work that you believe have been sent to you other than in accordance with this Privacy Policy, or breach of any law, please contact our Privacy Officer (contact details set out below). Our Privacy Officer will have your complaint reviewed and work with you to resolve it.

10. Access to and updating your personal information

You may request the details of any personal information we hold about you. Personal information held by HPA in respect of employees is subject to the "employee records exemption" under the Privacy Act and does not have to be disclosed on request. HPA may refuse to provide access to or delete information where this is required or authorised by the Privacy Act or another law.

If personal information is incorrect or incomplete, individuals may request that HPA amend its records and HPA will take reasonable steps to do so. On your request, and as far as it is practicable, we will also provide your updated details to third-party providers that we have previously disclosed your personal information with your consent.

11. Notification of data breach

If we experience a data breach, for example, unauthorised access to, or disclosure of, your personal information, or where your personal information is lost in circumstances that could give rise to unauthorised loss or disclosure, and serious harm is likely to occur to you, and we have not been able to prevent it we will advise you and the Australian Information Commissioner as soon as reasonably practical of the breach, and work with you to resolve it or mitigate the circumstances of the breach.

12. GDPR (for individuals within the European Union)

The GDPR provides data protection and privacy rights to individuals within the European Union as set out below.

Under the GDPR such individuals (you) are granted the following rights:

a) You have a right to know our identity. Please see 'Data Controller Details' at the end of this policy.

b) You may withdraw any given consent at any time.

c) You will be notified if, at any point in the future, the usage of your data changes from what is stated here. You will have the opportunity to withdraw consent.

d) You have the right to object to any of your data being processed.

e) You may request a copy of all information we have about you, at any time.

f) You may request modification of any data we have on you, at any time.

g) You may request deletion of any or all data we have on you, at any time

* For requests about your data, we will have to identify you to be able to comply.

Full details on your GDPR rights are provided at the following link:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

12.1 Data collection

Some personal data may be collected by us in the operation of our website. The amount of information collected depends on the level of interaction you have with us, such as signing up to the Support Centre or entering into competitions. Data we collect may include the following:

a) Identity data, such as name and email;

b) Contact information, such as email and phone number;

c) Financial and transactional data such as records of sales and purchases;

d) Usage data, such as email opening rates, number of website logins, etc;

e) Any other information you may volunteer to us, such as feedback or survey responses.

12.2 Cookies

We may use cookies on our website. You can set your browser to prevent this if you prefer. Cookies are stored in your browser, and may be deleted by you at any time.

12.3 Data usage

We will use your data for the following purposes:

a) To verify your identity should you wish to exercise your rights as above;

b) To provide information to you that you have requested;

c) To send you marketing and promotion materials and offers;

d) To generate anonymous aggregate data.

12.4 Recipients of data

Your data may be stored with third parties that provide services to us, such as our hosting provider and mailing list provider. Data may be available in some cases to contractors or associates that perform services for us, such as website development services.

12.5 Data retention

The period of data retention depends on the type of data, and the actions you take. We will retain data as long as is necessary to involve you in our work, or notify you of our events and activities, and may retain some information after your involvement with us ends. To have all information about you removed, please contact us, and we will comply as closely as allowed by law.

Please contact us (see details in Clause 14 below) if any of the following apply to you:

a) You want to know what data we have about you.

b) You want us to modify or delete any data we have about you.

c) You feel that your rights have not been met.

d) You do not understand any part of this policy.

e) You have unanswered questions about how we collect or use data.

12.6 Data breach

We will use best endeavours to report a personal data breach to the relevant supervisory authority within 72 hours of becoming aware of the breach, where feasible.

If the breach is likely to result in a high risk of adversely affecting your rights and freedoms, we will also inform you without undue delay.

Our Data Controller contact details are listed under Clause 14 below.

13. Website

The GDPR provides data protection and privacy rights to individuals within the European Union as set out below.

13.1 When you visit our website

When you visit our website www.hops.com.au, we will collect any personal information that you provide and we may collect certain information such as browser type, operating system, website visited immediately before coming to our site, etc. This information is used in an aggregated manner to analyse how people use our site so that we can improve our service.

13.2 Cookies

We may from time-to-time use cookies on our website. Cookies are very small files that a website uses to identify you when you come back to the site and to store details about your use of the site. Cookies are not malicious programs that access or damage your computer. Most web browsers automatically accept cookies, but you can choose to reject cookies by changing your browser settings. However, this may prevent you from taking full advantage of our website. Our website may from time to time use cookies to analyse website traffic and help us provide a better website visitor experience. By using our website you are assumed to consent to the use of cookies. In addition, cookies may be used to serve relevant ads to website visitors through third-party services such as Google AdWords. These ads may appear on this website or other websites you visit.

13.3 Third-party sites

Our site may from time to time have links to other websites not owned or controlled by us.

These links are meant for your convenience only. Links to third-party websites do not constitute sponsorship or endorsement or approval of these websites. Please be aware that HPA is not responsible for the privacy practices of other such websites. We encourage our users to be aware, when they leave our website, to read the privacy statements of every website that collects personal identifiable information.

14. Raising a concern or complaint

If you have any questions or concerns relating to this Policy or how we deal with your personal information, please discuss this with your manager, the hiring manager, or Head of People and Culture:

Kate Taylor
Phone: 0408 020 713
Email: kate.taylor@hops.com.au.

Alternatively, you may wish to contact HPA's nominated Data Controller:

Chris Price – Chief Financial Officer
Phone: 0408 326 052
Email: chris.price@hops.com.au

HPA will generally ask for your concern or complaint to be put in writing and it will endeavour to provide a prompt reply.

15. Responsibilities of management and employees

15.1 All employees must:

- Ensure full adherence to this Policy.
- Report all known or potential breaches of this Policy to your manager, the Managing Director, or the Data Controller;
- Strictly only access personal data if they need to do so for the proper performance of their role;
- Not share or communicate personal data unless this is necessary for the proper performance of their role;
- Keep personal data secure and protected, and under no circumstance share personal data or commercially sensitive HPA information on external AI-powered platforms such as ChatGPT;
- 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 when protecting documents with personal data on them;
- Lock unattended computer screens and devices;
- Never leave computers, devices, electronic storage systems, files, paperwork, or other things

containing personal data in a manner that risks unauthorised access or theft;

- Where appropriate and authorised to do so, ensure that highly sensitive personal data is encrypted before being transferred electronically to authorised external contacts;
- Consider anonymising data or using separate keys/codes so that the data subject cannot be identified;
- Not save personal employee data (other than own) to personal computers or other devices;
- Not take personal data away from HPA's premises unless required to do so for the proper performance of your role;
- Ask for help from your manager or IT team if unsure about data protection, or if any areas of data protection or security can be improved; and
- Immediately report any loss, unauthorised access, security risk, or other issues that arise in respect of personal information to your manager.

15.2 Additional responsibilities of managers and supervisors

- Monitor the working environment to ensure that acceptable standards are being observed.
- Behave in a manner consistent with the policy.
- Promote adherence to the policy.

16. Disciplinary action

Appropriate disciplinary action will be taken against a person who is found to have breached this policy. These measures will depend on the nature and circumstance of each breach and will be following the Discipline Policy.

In extreme circumstances, an individual may be concerned that a serious breach of this Policy has occurred but considers that it would be personally damaging to report it through normal channels, in such a case they should report it under the Speak Up (Whistleblowing) Policy.

17. Other policies

Employees are encouraged to read this policy in conjunction with other relevant HPA policies, including:

- Code of Conduct Policy
- Discipline Policy
- Discrimination, Bullying, and Harassment Policy
- Whistleblower (Speak Up) Policy
- Remote Working and Work from Home Policy

This policy was approved by the HPA Board on this date: 16/05/2023