Unily Australia Pty Ltd

Employee and Recruitment Privacy Notice

Unily Australia Pty Ltd ("Unily") is committed to the privacy of personal information in accordance with Australian privacy laws. This privacy notice applies to all current, former, and prospective employees, workers, and contractors of Unily.

It outlines how we collect and use your personal information before, during, and after your employment or engagement with us, and how we comply with the Australian Privacy Principles set out in the Privacy Act 1988 (Cth) as amended from time to time ('Privacy Act').

It is essential to read this notice along with any other privacy notice we provide on specific occasions when we collect or process your personal information so that you are aware of how and why we use it.

Our privacy notice is regularly reviewed to maintain transparency and accuracy. We encourage you to check it frequently for updates, and we will notify all staff of any significant changes.

Please note that this notice does not form part of any employment or service contract.

OUR PRIVACY PRINCIPLES

We are committed to complying with the Australian Privacy Principles and as part of this commitment, we ensure that your personal information is:

1. Used lawfully, fairly and in a transparent way.

2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.

3. Relevant to the purposes we have told you about and limited only to those purposes.

4. Accurate and kept up to date.

5. Kept only as long as necessary for the purposes we have told you about.

6. Kept securely.

THE KIND OF INFORMATION WE HOLD ABOUT YOU

Personal information means any information or an opinion about an identified individual, or an individual who is reasonably identifiable. It does not include data where a person's identity has been removed ("anonymous data").

The Privacy Act recognises that certain categories of personal information are more sensitive and require a higher level of privacy protection. This is referred to as "sensitive information".

We may collect, store, and use the following categories of personal information:

- Your name, contact details (i.e. address, home and mobile phone numbers, email address) and emergency contacts (i.e. name, relationship and home and mobile phone numbers);
- Information collected during the recruitment process that we retain during your employment;
- Employment contract information;
- Details of salary and benefits, bank/building society, National Insurance and tax information, your age;
- Details of your spouse/partner and any dependants;
- Next of kin and emergency contact details;
- Your nationality and immigration status and information from related documents, such as your passport or other identification and immigration information;
- A copy of your driving licence; passport;
- Details of your share incentive arrangements, and all information included in these and necessary to implement and administer them, if applicable;
- Details of your superannuation arrangements, and all information included in these and necessary to implement and administer them;
- Information on your sickness and absence records;
- Information on grievances raised by or involving you;
- Information on conduct and/or other disciplinary issues involving you;
- Details of your appraisals and performance reviews;
- Details of your performance management/improvement plans (if any);
- Details of your time and attendance records;
- Information regarding your work output;
- Information in applications you make for other positions within our organisation;
- Information about your use of our IT, communication and other systems, and other monitoring information;
- Details of your use of business-related social media, such as LinkedIn;
- Your use of public social media (only in very limited circumstances, to check specific risks for specific functions within our organisation; you will be notified separately if this is to occur); and
- Details in references about you that we give to others;
- Photographs.

We may also collect, store and use the following types of sensitive personal information:

- Diversity, equity and inclusion (DE&I) data (such as gender, health, ethnicity, race, disability, sexual orientation, religion, and socioeconomic background) where permitted by law and provided voluntarily by you as part of any DE&I questionnaire;
- Information about your health, including any medical condition, health and sickness records, including:
    - where you leave employment and under any share plan operated by a group company the reason for leaving is determined to be ill-health, injury or disability, the records relating to that decision;

    - details of any absences (other than holidays) from work including time on statutory parental leave and sick leave; and
    - where you leave employment and the reason for leaving is related to your health, information about that condition needed for superannuation and permanent health insurance purposes.
- Information about criminal convictions and offences.

Certain categories above may not apply to you if you are an agency worker, independent contractor, freelancer, volunteer, intern, or a member of the Executive Leadership Team.

HOW YOUR PERSONAL INFORMATION IS COLLECTED

We typically collect personal information about employees, workers and contractors through the application, recruitment and on-boarding process, either directly from candidates or sometimes from an employment agency. We will also collect additional information from third parties including former employers and background check agencies.

We will collect additional personal information in the course of job-related activities throughout the period of you working for us. This will include your information from your line manager (for example, in respect of performance reviews) or, from time to time, from other managers or colleagues (for instance, in the course of conducting an investigation).

We may also receive personal information from other third parties, for example clients, tax authorities, benefit providers, brokers and regulatory bodies to the extent permitted by applicable laws.

Use of CCTV

We use CCTV in and around our buildings to maintain the security of property, premises, and staff, and for the prevention and detection of crime. For these reasons, personal information may be collected through the means of CCTV, including visual images, and information revealing personal appearance or behaviours.

HOW WE WILL USE INFORMATION ABOUT YOU

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

1. Making a decision about your recruitment or appointment;

2. Where it is necessary for the performance of the employment contract we have entered into with you, or to take steps to enter into a contract;

3. Where we need to comply with a legal obligation;

4. Where it is necessary for our legitimate interests (or those of a third party) and

your interests and fundamental rights do not override those interests.

We may also use your personal information in the following situations, which are likely to be rare:

1. Where we need to protect your interests (or someone else's interests);

2. Where it is needed in the public interest or for official purposes.

Situations in which we will use your personal information

We need all the categories of personal information in the list above (see *The kind of information we hold about you*) primarily to allow us to perform our contract with you and to enable us to comply with legal obligations. We also use your personal information to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights do not override those interests.

The situations in which we will process your personal information are listed below. As demonstrated, some of the below grounds for processing overlap and there may be several grounds which justify our use of your personal information.

Purpose	**Justification**
Recruitment and selection, including but not limited to processing of the personal information included in CVs, references, interview sheets, pre-employment forms, and results from assessment tests.	The processing is necessary for the purpose of the **legitimate interests** pursued by Unily, in ensuring that only suitable and appropriate candidates are assessed, shortlisted and selected.
Appropriate vetting and background checks for recruitment and team allocation including, right to work verification, relevant employment or engagement history, academic/education checks and professional qualifications and bringing you on-board and creating an employment record.	The processing is necessary for the compliance with **legal obligations** to which Unily is subject. The processing is also necessary to take steps at the applicant's request to **enter a contract** of employment.
Providing and administering remuneration, bonus and pension schemes, benefits and incentive schemes and reimbursement of business costs and expenses and making appropriate pension, tax and social security deductions and contributions;	The processing is necessary to **perform the contract** between you and Unily and necessary for compliance with legal obligations.
General employee management, including: • allocating and managing duties and responsibilities and the business activities to which they relate; • planning and allocating work and measuring working hours;	The processing is necessary to perform the **contract** between you and Unily and, where necessary, for compliance with legal obligations. The processing is also necessary for the

Purpose	Justification
• providing and managing annual leave and business travel; • managing flexible working/part-time arrangements/time sheets/attendance records of employees; • maintaining emergency contact and beneficiary details; • managing health and safety at work and investigate and report on incidents/accidents.	purpose of the **legitimate interests** pursued by Unily. Unily considers that it has a legitimate interest in managing its workforce and ensuring that each employee undertakes appropriate duties, are properly trained and undertake their roles correctly and in accordance with appropriate procedures.
Identifying and communicating effectively with employees, including managing internal directories to facilitate contact and effective working and communication;	The processing is necessary for the purpose of the **legitimate interests** pursued by Unily. Unily considers that it has a legitimate interest in undertaking normal business operations and maintaining a dialogue with employees to ensure effective management and job satisfaction.
Managing and operating appraisal, conduct, performance, capability, behavioural, absence and grievance related reviews, allegations, complaints, investigations and processes and other informal and formal HR and legal compliance processes and making related management decisions;	The processing is necessary to **perform the contract** between you and Unily and for the compliance with legal obligations to which Unily is subject. The processing is also necessary for the purpose of the **legitimate interests** pursued by Unily. Unily considers that it has a legitimate interest in addressing employee related concerns and issues and resolving the same and complying with applicable laws and regulations.
Training, development, promotion, career and succession planning and business contingency planning;	The processing is necessary to **perform the contract** between you and Unily. The processing is also necessary for the purpose of the **legitimate interests** pursued by Unily. Unily considers that it has a legitimate interest in effective employee management to support its long-term business goals and outcomes to ensure it continues to retain as well as attract high calibre employees.
Processing information about absence or medical information regarding physical or mental health or	The processing is necessary for the compliance with **legal obligations** to

Purpose	Justification
condition in order to: • assess eligibility for incapacity or permanent disability related remuneration or benefits; • determine fitness for work; • facilitate a return to work; • make reasonable adjustments or accommodations to duties or the workplace; • make management decisions regarding employment or engagement or continued employment or engagement or redeployment; • and conduct related management processes;	which Unily is subject. The processing is also necessary for the purpose of the **legitimate interests** pursued by Unily. Unily considers that it has a legitimate interest in ensuring that employee undertakes appropriate duties, are properly trained, supported by management and undertake their roles correctly and in accordance with appropriate procedures.
Complying with reference requests where Unily is named by the individual as a referee;	This processing is necessary for the purpose of the **legitimate interests** pursued by Unily. Unily considers that it is in the legitimate interests of a new employer to receive confirmation of employment or engagement details from Unily for the purposes of confirming the former employee's employment or engagement history.
Operating email, IT, internet, social media, HR related and other company policies and procedures. To the extent permitted by applicable laws, Unily carries out monitoring of Unily's IT systems to protect and maintain the integrity of Unily's IT systems and infrastructure; to ensure compliance with Unily's IT policies and to locate information through searches where needed for a legitimate business purpose;	The processing is necessary to **perform the contract** between you and Unily and for the compliance with legal obligations to which Unily is subject. The processing is also necessary for the purpose of the **legitimate interests** pursued by Unily. Unily considers that it has a legitimate interest in managing its workforce and operating its business through IT systems. The HR IT function is essential to ensuring that this can be carried out in the most effective way.
Protecting the private, confidential and proprietary information of Unily, its employees, clients and third parties and protecting the security of our sites, systems, employees and visitors e.g. through the use of CCTV;	The processing is necessary for the compliance with **legal obligations** to which Unily is subject. The processing is also necessary for the purpose of the **legitimate interests** pursued by Unily. Unily considers that it has a legitimate interest in ensuring that its business, clients, employees and systems are protected. This includes

Purpose	Justification
	protecting our assets and the integrity of our systems; and detecting and preventing loss of our confidential information and proprietary information.
Complying with applicable laws and regulations (for example, maternity or parental leave legislation, working time and health and safety legislation, taxation rules, worker consultation requirements, other employment laws and regulations);	The processing is necessary for the compliance with **legal obligations** to which Unily is subject.
Planning, due diligence and implementation in relation to a commercial transaction or service transfer involving Unily that impacts on your relationship with Unily for example mergers and acquisitions or a transfer of your employment under applicable automatic transfer rules;	The processing is necessary for the compliance with **legal obligations** to which Unily is subject. This processing is also necessary for the purpose of the **legitimate interests** pursued by Unily. Unily needs to make decisions relating to the future of its business in order to preserve its business operations or grow its business.
Where relevant, for publishing (including via social media in appropriate circumstances) internal or external communications or publicity material;	The processing is necessary for the purpose of the **legitimate interests** pursued by Unily. Unily considers that it has a legitimate interest to support its long-term business goals and outcomes and Unily wishes to maintain its reputation. **Note**: employees' will be provided with the opportunity to opt out.
To support HR administration and management and maintaining and processing general records necessary to manage the employment, employees or other relationship and operate the contract of employment or engagement;	The processing is necessary to **perform the contract** between you and Unily and for the compliance with **legal obligations** to which Unily is subject. The processing is also necessary for the purpose of the **legitimate interests** pursued by Unily. Unily considers that it has a legitimate interest in effective employee management to support its long-term business goals and outcomes.
To enforce our legal rights and obligations, and for any purposes in connection with any legal claims, reports of violations or allegations made by, against	The processing is necessary for the purpose of the **legitimate interests** pursued by Unily. Unily considers that it

Purpose	Justification
or otherwise involving you.	has a legitimate interest in protecting its organisation from breaches of legal obligations owed to it and defending itself against litigation. This is needed to ensure that Unily's legal rights and interests are protected appropriately, to protect Unily's reputation and to protect Unily from other damage or loss. The processing is also necessary for the compliance with **legal obligations** to which Unily is subject.
To collect and monitor DE&I data in order to foster a more equitable, inclusive, and supportive workplace. This includes identifying underrepresented groups, addressing barriers to inclusion in recruitment and career progression, implementing targeted initiatives to attract and retain diverse talent, and ensuring fair, unbiased hiring practices that provide equal opportunity for all candidates.	Participation in DE&I questionnaires is entirely voluntary and **based on consent**. Respondents may choose how much information to share, and all responses will be treated in the strictest confidence and used solely for statistical monitoring purposes. The provision or non-provision of this information will have no impact on an individual's application, and hiring managers will not have access to identifiable DE&I data.
The use of employee photographs for internal business purposes, to generate employee engagement within the workplace.	The processing is necessary for the purpose of the **legitimate interests** pursued by Unily. Unily considers that it has a legitimate interest in generating employee engagement within the workplace as part its efforts to maintain employee motivation, satisfaction, and retention levels. **Note**: employees' will be provided with the opportunity to opt out.
Recording, transcribing, and analysing calls involving sales staff to support internal training and coaching initiatives. This includes facilitating peer-to-peer coaching, identifying areas for improvement, providing personalised feedback, and ensuring adherence with company standards and best practices.	The processing is necessary for the purpose of the **legitimate interests** pursued by Unily. Unily considers that it has a legitimate interest in improving customer and prospect interactions, increasing sales effectiveness, and fostering the professional development of our employees.

Please note that this not an exhaustive list and we may process your data for other purposes that are consistent with the purposes for which your personal information is

primarily held or for a related secondary purpose. Further, additional information regarding specific processing of personal information may be notified to you locally or as set out in applicable policies.

If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers). Where we ask you to provide personal information to us on a mandatory basis, we will inform you of this at the time of collection and in the event that particular information is required by the contract or statute this will be indicated.

Change of purpose

We will only use your personal information for the primary purposes for which we collected it, unless we reasonably consider that we need to use it for another secondary purpose and that reason is compatible with the primary purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal justification which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

HOW WE USE SENSITIVE PERSONAL INFORMATION

We recognise that sensitive personal information requires a higher level of protection. As such, we will only process this type of personal information where it is strictly necessary for us to collect, store, and use it.

For example, we may process sensitive personal information in the following circumstances:

1. Where we have obtained your consent;

2. Where we need to carry out our legal obligations or exercise rights in connection with employment;

3. Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our occupational superannuation scheme;

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent.

Our obligations as an employer

We will use sensitive personal information in the following ways:

- We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws.
- We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits including statutory parental leave pay, statutory sick pay, superannuation and permanent health insurance.
- We will use information about isolation notices, testing results and vaccination records to ensure health and safety in the workplace and to monitor and limit the chance of infection, where permitted to do so by law.
- We will use your DE&I data, where provided by you voluntarily, to ensure meaningful equal opportunity monitoring and reporting.

Do we need your consent?

In certain circumstances, will be required to approach you for your written consent to allow us to process your sensitive personal information, where required under the Privacy Act. Where we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

INFORMATION ABOUT CRIMINAL CONVICTIONS

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our legal obligations in connection with employment law.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where it is necessary for preventing or detecting unlawful acts.

Our appropriate policy document provides further information about this processing.

- We will use information in connection with any criminal convictions or offences to enable Unily to assess your suitability for employment. We will also process and share such data with relevant authorities should any criminal activity take place in connection within the workplace.

DATA SHARING

We will share your data with third parties, including third-party service providers and other entities in the group.

We require third parties to respect the security of your personal information and to treat it in accordance with the law.

Information may be transferred internationally to other countries around the world, including countries that do not have data protection laws equivalent to those in Australia. If we do, we will take steps to ensure that your personal information is adequately protected.

Why might you share my personal information with third parties?

We may share your personal information with third parties for the purposes for which it is primarily held or for a related secondary purpose, including: (i) where required by law, regulation or legal process (such as a court order or subpoena); (ii) where it is necessary to administer the working relationship with you; (iii) in response to lawful requests by government agencies; or (iii) where we have another legitimate interest in doing so. In some cases, we may only disclose information with your consent.

What sort of third-parties might my personal information be shared with?

The following are examples of third-parties with whom personal information about you may to be shared with:

- Governmental departments, statutory and regulatory bodies including the Office of the Australian Information Commissioner, Australian Taxation Office, and Safe Work Australia to meet statutory reporting obligations;
- Background check providers;
- Employment-related benefits providers and other third parties in connection with your benefits (such as your pension, health insurance provider etc.);
- Payroll/tax providers;
- Law enforcement agencies for the prevention or detection of crime;
- External auditors, insurers, investors and lenders;
- Medical/occupational health professionals;
- Consultants and other professional advisors (such as lawyers, accountants etc.),
- Emergency response services as necessary to protect your vital interests or those of another person;
- IT service providers, such as those responsible for hosting, supporting and maintaining the framework of Unily's information systems (including our HR systems);
- Landlords and office access providers;
- Social media and marketing suppliers;
- Employee learning and development providers.

How secure is my personal information with third-party service providers and other entities in our group?

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our Data Protection Policy. We do not allow our third-party service providers to use your personal information for their own purposes. We only permit them to process your personal information for specified purposes and in accordance with our instructions.

When might you share my personal information with other entities in the group?

We will share your personal information with other entities in our group, including Unily Inc (USA) and Unily Group Limited (UK) where required to, for example, run global processes, carry out group wide reporting, and assist with workforce planning.

Transferring information outside Australia

The global nature of our business means that your personal information will routinely be shared with other entities in our group outside of Australia, namely in the USA and UK. Unily has an intra-group data transfer agreement in place which regulates cross-border transfers of your personal information within the group.

Certain suppliers and service providers may also have personnel or systems located outside of Australia, including in the European Union, United States and United Kingdom. As a result, your personal information may be transferred to countries outside of the country in which you work, and the laws in those countries may not offer a level of protection of personal information equivalent to that offered within Australia. Where third parties process your personal information outside of Australia, we will take steps to ensure that your data receives an adequate level of protection, including by, for example, entering into data transfer agreements or by ensuring that third parties are certified under appropriate data protection schemes.

DATA SECURITY

We have put in place measures to protect the security of your personal information. Details of these measures are available upon request.

Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have implemented appropriate security measures to prevent unauthorised access, alteration, disclosure, or accidental loss of your personal information. Only authorised employees, agents, contractors, and third parties with a business need to know will have access to your personal information, and they are subject to a duty of confidentiality.

We have an Incident Management Policy that outlines the process for investigating, managing, and resolving incidents, which are monitored by the Information Security Manager and the Data Protection Officer. In the event of a personal information breach occurring that impacts you, we will notify you and any relevant regulatory authorities where legally required to do so.

DATA RETENTION

How long will you keep my personal information for?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. To determine the appropriate retention period for personal information, we consider the amount, nature, and sensitivity of the personal information, the potential risk of harm from unauthorised use or disclosure of your personal information, the purposes for which we process your personal information and whether we can achieve those purposes through other means, and the applicable legal requirements.

Retention periods can vary depending on why we need your data, including as set out below:

Record Type	Retention Period
Payroll wage/salary records (including overtime, bonuses, expenses)	7 years post-employment.
Income tax returns, income tax records and correspondence with tax and related authorities	7 years post-employment
Employee file data	7 years post-employment* *data may be retained beyond its retention period in limited circumstances such as to raise, defend, continue litigation or other dispute resolution process or for insurance reasons.
Recruitment data – successful candidates	7 years post-employment
Recruitment data – unsuccessful candidates	6 months post-campaign

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker or contractor of the company we will retain and securely destroy your personal information in accordance with our retention schedule.

RIGHTS OF ACCESS AND CORRECTION

Your duty to inform us of changes

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

Your rights in connection with personal information

Under the Privacy Act, you are entitled to:

- **Request access** to your personal information we hold about you. This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.

If you wish to request access to or the erasure of your personal information, please contact the Data Protection Officer using the contact details provided below.

No fee usually required

We will not charge you for processing a request to correct your personal information. Equally, you will not generally have to pay a fee to access your personal information. However, in certain circumstances, such as if your access request is particularly complex or voluminous, a small administrative fee may be payable to cover our expenses in dealing with the request.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access or correct the information. This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it or amended by an unauthorised person.

DATA PROTECTION OFFICER

We have appointed a Data Protection Officer to oversee Unily's privacy compliance. If you have any questions or concerns about this privacy notice or our privacy practices, the Data Protection Officer and wider Data Protection Team can be contacted at privacy@unily.com.

If you have a complaint, we will investigate the issue and ensure it is handled in an appropriate and reasonable manner. Where necessary, we may consult with our related entities and partners in order to deal with your complaint. A written notice of our decision regarding your complaint will be provided to you.

If you are not satisfied with the outcome, then you may contact the Office of the Australian Privacy Commissioner:

Office of the Australian Information Commissioner
Website: www.oaic.gov.au
Phone: 1300 363 992

CHANGES TO THIS PRIVACY NOTICE

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

Classification: Public

Last Updated: 08.04.25