

## Unily Group Limited

### Employee and Recruitment Privacy Notice

Unily Group Limited ("Unily") is the controller of your personal information and is committed to protecting the privacy and security of your data. 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 your associated rights, in accordance with the UK General Data Protection Regulation (GDPR).

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.

#### DATA PROTECTION PRINCIPLES

We are committed to complying with data protection law and ensuring 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, referred to throughout the rest of this notice as "personal data", means any information about an individual from which that person can be identified. It does not include data where a person's identity has been removed ("anonymous data").

The law recognises that certain categories of personal data are more sensitive and require a higher level of protection. These are referred to as "special categories" of personal data.

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

- Contact details, including name, address, telephone number and personal e-mail address, as well as next of kin details;
- Information and references collected during the recruitment process, relating to your education and employment history;
- Information about your right to work in the UK and copies of proof of right to work documentation, such as your passport, visa, birth certificate or other identity documentation;
- Details of terms and conditions of employment, including pay and benefits;
- Payroll, tax, pension and NI information;
- Performance information;
- Details of grades and job duties;
- Absence, self-certification forms and holiday records;
- Details of disciplinary investigations and proceedings;
- Details of grievance investigations and proceedings;
- Minutes from meetings attended;
- Details of expenses and travel;
- Training records;
- Correspondence with the Unily and other information provided by you to Unily during the course of your employment;
- Details of websites visited using company-provided internet access, emails and messages sent and received and other correspondence, and details of work-related social media, e.g. LinkedIn;
- Data generated in relation to your location, use of electronic devices and travelling;
- Photographs and pictures of you from events and on-site CCTV footage at Unily office locations;

We may also collect, store and use the following special categories of personal data:

- Information regarding your health, for the purposes of complying with our health and safety and occupational health obligations. This may include details on testing and vaccination data where required in connection with public health laws, regulations relating to the control of infectious diseases or pandemics, or other applicable requirements imposed on Unily. Such information may also be used to support management decisions relating to your ability to perform your role, to determine whether reasonable adjustments are necessary to assist you with a disability, and for the administration of insurance, pension, sick pay, and other related benefits in force from time to time;
- Diversity, equity, and inclusion (DE&I) data (such as gender, health, ethnicity, race, disability, sexual orientation, religion and socioeconomic background) voluntarily provided by you as part of any DE&I questionnaire;
- Data collected in connection with necessary employment background checks, including criminal records checks from the Disclosure and Barring Service, to enable Unily to assess your suitability for employment.

## **HOW YOUR PERSONAL DATA IS COLLECTED**

We typically collect personal data about employees, workers and contactors 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 data 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 data 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 data 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 data when the law allows us to. Most commonly, we will use your personal data in the following circumstances:

1. Where it is necessary for the performance of a contract we have entered with you, or to take steps to enter into a contract (such as your contract of employment);
2. Where we need to comply with a legal obligation;
3. 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 data 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 data**

We need all the categories of personal data 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 data 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 data 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 data.

Purpose	Legal Basis
Recruitment and selection, including but not limited to processing of the personal data included in CVs, references, interview sheets, pre-employment forms, and results from assessment tests.	The processing is necessary for the purpose of the <b>legitimate interests</b> 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.	<p>The processing is necessary for the compliance with <b>legal obligations</b> to which Unily is subject.</p> <p>The processing is also necessary to take steps at the applicant's request to <b>enter a contract</b> of employment.</p>
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 <b>perform the contract</b> between you and Unily and necessary for compliance with legal obligations.
<p>General employee management, including:</p> <ul style="list-style-type: none"> <li>• allocating and managing duties and responsibilities and the business activities to which they relate;</li> <li>• planning and allocating work and measuring working hours;</li> <li>• providing and managing annual leave and business travel;</li> <li>• managing flexible working/part-time arrangements/time sheets/attendance records of employees;</li> <li>• maintaining emergency contact and beneficiary details;</li> <li>• managing health and safety at work and investigate and report on incidents/accidents.</li> </ul>	<p>The processing is necessary to perform the <b>contract</b> between you and Unily and, where necessary, for compliance with legal obligations.</p> <p>The processing is also necessary for the purpose of the <b>legitimate interests</b> 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.</p>
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 <b>legitimate interests</b> 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

Purpose	Legal Basis
	satisfaction.
<p>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;</p>	<p>The processing is necessary to <b>perform the contract</b> between you and Unily and for the compliance with legal obligations to which Unily is subject.</p> <p>The processing is also necessary for the purpose of the <b>legitimate interests</b> 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.</p>
<p>Training, development, promotion, career and succession planning and business contingency planning;</p>	<p>The processing is necessary to <b>perform the contract</b> between you and Unily.</p> <p>The processing is also necessary for the purpose of the <b>legitimate interests</b> 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.</p>
<p>Processing information about absence or medical information regarding physical or mental health or condition in order to:</p> <ul style="list-style-type: none"> <li>• assess eligibility for incapacity or permanent disability related remuneration or benefits;</li> <li>• determine fitness for work;</li> <li>• facilitate a return to work;</li> <li>• make reasonable adjustments or accommodations to duties or the workplace;</li> <li>• make management decisions regarding employment or engagement or continued employment or engagement or redeployment;</li> <li>• and conduct related management processes;</li> </ul>	<p>The processing is necessary for the compliance with <b>legal obligations</b> to which Unily is subject.</p> <p>The processing is also necessary for the purpose of the <b>legitimate interests</b> 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.</p>
<p>Complying with reference requests where Unily is named by the individual as a referee;</p>	<p>This processing is necessary for the purpose of the <b>legitimate interests</b> pursued by Unily. Unily considers that it is in the legitimate interests of a new employer to receive confirmation of</p>

Purpose	Legal Basis
	employment or engagement details from Unily for the purposes of confirming the former employee's employment or engagement history.
<p>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;</p>	<p>The processing is necessary to <b>perform the contract</b> between you and Unily and for the compliance with legal obligations to which Unily is subject.</p> <p>The processing is also necessary for the purpose of the <b>legitimate interests</b> 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.</p>
<p>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;</p>	<p>The processing is necessary for the compliance with <b>legal obligations</b> to which Unily is subject.</p> <p>The processing is also necessary for the purpose of the <b>legitimate interests</b> pursued by Unily. Unily considers that it has a legitimate interest in ensuring that its business, clients, employees and systems are protected. This includes protecting our assets and the integrity of our systems; and detecting and preventing loss of our confidential information and proprietary information.</p>
<p>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);</p>	<p>The processing is necessary for the compliance with <b>legal obligations</b> to which Unily is subject.</p>
<p>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;</p>	<p>The processing is necessary for the compliance with <b>legal obligations</b> to which Unily is subject.</p> <p>This processing is also necessary for the purpose of the <b>legitimate interests</b> pursued by Unily. Unily needs to make</p>

Purpose	Legal Basis
	<p>decisions relating to the future of its business in order to preserve its business operations or grow its business.</p>
<p>Where relevant, for publishing (including via social media in appropriate circumstances) internal or external communications or publicity material;</p>	<p>The processing is necessary for the purpose of the <b>legitimate interests</b> 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.</p> <p><b>Note:</b> employees' will be provided with the opportunity to opt out.</p>
<p>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;</p>	<p>The processing is necessary to <b>perform the contract</b> between you and Unily and for the compliance with <b>legal obligations</b> to which Unily is subject.</p> <p>The processing is also necessary for the purpose of the <b>legitimate interests</b> pursued by Unily. Unily considers that it has a legitimate interest in effective employee management to support its long-term business goals and outcomes.</p>
<p>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 or otherwise involving you.</p>	<p>The processing is necessary for the purpose of the <b>legitimate interests</b> pursued by Unily. Unily considers that it 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.</p> <p>The processing is also necessary for the compliance with <b>legal obligations</b> to which Unily is subject.</p>
<p>To collect and monitor DE&amp;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,</p>	<p>Participation in DE&amp;I questionnaires is <b>entirely voluntary</b>. Respondents may choose how much information to share, and all responses will be treated in the strictest confidence and used solely for</p>

Purpose	Legal Basis
implementing targeted initiatives to attract and retain diverse talent, and ensuring fair, unbiased hiring practices that provide equal opportunity for all candidates.	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. For those who choose to participate, the processing is carried out on the basis of Unily's <b>legitimate interests</b> . Unily considers that it has a legitimate interest in monitoring and promoting equal opportunities throughout the recruitment process and within the workplace. This also supports Unily's efforts to comply with its <b>legal obligations</b> in this regard.
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 <b>legitimate interests</b> 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. <b>Note:</b> 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 <b>legitimate interests</b> 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 legal basis on which we process your personal data. Further, additional information regarding specific processing of personal data may be notified to you locally or as set out in applicable policies.

### **If you fail to provide personal data**

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

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

## **HOW WE USE SPECIAL CATEGORY PERSONAL DATA**

As the law requires that special category personal data is provided a higher level of protection, we need to have further justification for collecting, storing, and using this type of personal data. We may process special categories of personal data in the following circumstances:

1. Where we need to carry out our legal obligations, such as those in connection with employment, social security, and social protection law.
2. Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.

In addition, we rely on the processing condition at Schedule 1 part 1 paragraph 1 of the Data Protection Act 2018. This relates to the processing of special category data for employment purposes. Our appropriate policy document provides further information about this processing.

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, or where you have already made the information public.

### **Our obligations as an employer**

We will use special category personal data 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.
- 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, provided voluntarily, to ensure meaningful equal opportunity monitoring and reporting.

### **Do we need your consent?**

We do not need your consent if we use special categories of personal data in accordance with our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If 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 you have already made the information public.

We also rely on the processing condition at Schedule Part 2 paragraph 10 - preventing or detecting unlawful acts under the Data Protection Act 2018. 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 data and to treat it in accordance with the law.

We may transfer your personal data outside the UK and EEA.

If we do, you can expect a similar degree of protection in respect of your personal data.

### **Why might you share my personal data with third parties?**

We may share your personal data with third parties (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.

### **What sort of third-parties might my personal data be shared with?**

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

- Governmental departments, statutory and regulatory bodies including the Department for Work & Pensions, Information Commissioner's Office, Her Majesty's Revenue and Customs (HMRC) or Health and Safety Executive (HSE) 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 data 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 data in line with our Data Protection Policy. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

### **When might you share my personal data with other entities in the group?**

We will share your personal data with other entities in our group, including Unily Inc (US) and Unily Pty Ltd (Australia) where required to, for example, run global processes, carry out group wide reporting, and assist with workforce planning.

## **Transferring information outside the UK and EEA**

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

Certain suppliers and service providers may also have personnel or systems located outside of the UK and EEA. As a result, your personal data may be transferred to countries outside of the country in which you work to countries that may not offer a level of protection of personal data equivalent to that offered within the UK and EEA. Where third parties process your personal data outside of the UK and EEA, 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.

You have a right to request a copy of any data transfer agreement under which your personal data is transferred, or to otherwise have access to the safeguards used by contacting us. Any data transfer agreement made available to you may be redacted for reasons of commercial sensitivity.

## **DATA SECURITY**

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

Third parties will only process your personal data 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 data. Only authorised employees, agents, contractors, and third parties with a business need to know will have access to your personal data, 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 data 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 data for?**

We will only retain your personal data 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

data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data 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, as set out below:

Record Type	Retention Period
Payroll wage/salary records (including overtime, bonuses, expenses)	7 years post-employment.
Income tax and NI returns, income tax records and correspondence with HMRC	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 data 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 data in accordance with our data protection policy.

## **RIGHTS OF ACCESS, CORRECTION, ERASURE, AND RESTRICTION**

### **Your duty to inform us of changes**

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

### **Your rights in connection with personal data**

Under certain circumstances, by law you have the right to:

- **Request access** to your personal data (commonly known as a “subject access request”). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal data that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have exercised your right to object to processing (see below).
- **Object to processing** of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal data for direct marketing purposes.
- **Request the restriction of processing** of your personal data. This enables you to ask us to suspend the processing of personal data about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of your personal data to another party.

If you want to review, verify, correct, or request erasure of your personal data, object to the processing of it, or request that we transfer a copy of your personal data to another party, please contact the Data Protection Officer using the contact details below.

### **No fee usually required**

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

### **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 the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal data is not disclosed to any person who has no right to receive it.

## **DATA PROTECTION OFFICER**

We have appointed a Data Protection Officer to oversee Unily’s data protection compliance. If you have any questions about this privacy notice or how we handle your personal data, the Data Protection Officer and wider Data Protection Team can be contacted at [privacy@unily.com](mailto:privacy@unily.com).

If you believe that we have complied with your data protection rights, you also have the right to complain to the Information Commissioner’s Office (ICO), the UK supervisory

authority for data protection issues, using their help line 0303 123 1113 or visit their website.

## **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 data.

**Classification: Public**

**Last Updated: 08.04.25**