Dated: 31st May 2023

RECRUITMENT PRIVACY POLICY

1. INTRODUCTION

The Data Protection Act 2018 ("**the Act**") sets out the principles that all companies within the Argonon Group must follow when processing personal data about individuals, and also gives individuals certain rights in relation to personal data that is held about them.

The Argonon Group consists of Argonon Limited, and all subsidiary companies (collectively, ("**the Company**", "**we**", "**our**", "**us**"). Click here for a full list of companies within the Argonon Group.

We are the data controller in respect of any personal data. This means that we are required under UK data protection legislation (including the Act) to notify you of how we will process your personal data during the recruitment process.

This policy lets you know how we will fulfil our obligations under the Act when you send us your CV or apply for work with any of our companies; setting out how we collect your personal data, its use, storage, transfer and security. We will also explain what rights you have in relation to how we process your personal data.

It is important that you read this policy, together with any other privacy policy/notice we may provide during the recruitment process, so that you are aware of how and why we are processing your personal data.

The terms "**applicant(s)**", "**you**" or **"your**", will be used in this policy to refer to anyone who applies for a job role, or who otherwise seeks to carry out work with or for us (whether on a permanent or non-permanent basis).

We may update this policy at any time.

2. DATA PROTECTION PRINCIPLES & OUR OBLIGATIONS TO YOU

The following key principles underpin the Company's approach when processing personal data:

1. **Manner of collection:** personal data, in relation to individuals, must be processed lawfully, fairly and in a transparent manner.

2. **Uses of what is collected:** personal data must be collected only for specified, explicit, valid and legitimate purposes that we have clearly explained to you and not used or processed in any way that is incompatible with those purposes.

3. **How personal data is collected:** personal data which is collected must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is being processed.

4. **Managing what is collected:** personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data which is inaccurate (having regard to the purposes for which it is processed) is erased or rectified without delay.

5. **How long to keep what is collected**: personal data must be kept in a form which permits individuals to be identified for only as long as necessary for the purposes for which the data is processed.

6. **Securing what is collected:** personal data must be processed in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

We are responsible for and must be able to demonstrate compliance with these principles in our processing of personal data.

"Processing" is the term used in the Act to refer to a wide range of activities in relation to personal data including its collection, retention, use, disclosure, and final destruction or erasure.

3. WHAT PERSONAL DATA WILL WE COLLECT, USE AND STORE ABOUT YOU?

During the recruitment process, we may collect, hold and process certain data, categorised as follows:

Personal data – is information relating to an identifiable person, and includes:

- Your name, addresses, contact numbers, and personal email addresses.
- Date of birth.
- Gender.
- Employment history.
- Qualifications.
- Interests.
- Recruitment information (including copies of right to work documentation, previous applications you have made, references and other information included in your CV or cover letter or shared as part of the application process).

Special category data – is personal data that needs more protection because it is sensitive, and includes:

- Information about your race or ethnicity, disability, religious beliefs, sexual orientation, and political opinions. We may, for example, use race and ethnic origin data to monitor our equal opportunities diversity policy. Such data will, where applicable, be anonymised.

- Biometric data (for identification and right to work check purposes). During the recruitment process you will, if we make an offer of employment, be asked to conduct a right to work check. This will typically be undertaken via a digital identity service provider ("**IDSPs**"), who will (in accordance with our instructions) collect, store and process biometric data contained within your identification documents (e.g., Passport). We will have the ability to access and export this data from the IDSP; storing it within our HR and Payroll systems.

Criminal offence data – includes personal data about criminal allegations, proceedings or convictions and related security measures. We rarely process this category of data. Examples of when we do include undertaking DBS checks for production teams who work with children, and in other safeguarding scenarios.

Some of the above information may be obtained from you or from third party recruitment platforms (e.g., Talentbase, Talent Manager, LinkedIn) and via recruitment agencies.

Information about you may be verified by: (i) performing background checks, including using information posted by you on your publicly available social media platforms; (ii) checks obtained lawfully from third parties engaged by us for verification purposes such as data intelligence services and any organisation authorised to provide basic criminal history checks; and (iii) (at our request) providing us with documentation to verify your personal information.

We regularly monitor guidance from the Information Commissioner's Office (https://ico.org.uk/) and industry specific guidance from PACT (https://www.pact.co.uk/) with respect to special category and criminal offence data and will amend this policy (as necessary) in the event updates are published.

Dated: 31st May 2023

4. HOW WILL WE USE YOUR PERSONAL DATA?

We process personal information for the following purposes:

- to communicate with you about your application or the recruitment process;
- to analyse and monitor the diversity of our applicants in accordance with applicable laws;
- to undertake right to work checks (when an offer of employment is made as part of the recruitment process);
- to undertake verification checks on background and references;
- for our HR records;
- to assess skills, qualifications and suitability for available work.

Our legal basis for processing your personal information, as part of the recruitment process, will be:

- to pursue our legitimate interests in seeking suitable candidates for available work;
- to take steps prior to entering into a contract with you, where you are considered for a role;
- to obtain your consent to use your sensitive personal information (e.g., where collected as part of right to work checks);
- to ensure we can comply with our legal and regulatory obligations (i.e., applicable immigration and/or employment laws and regulations).

At all times Argonon will ensure that the lawful basis for processing personal data will not override the interests, rights and freedoms of individuals.

5. WHAT HAPPENS IF WE NEED TO USE YOUR PERSONAL DATA FOR A NEW PURPOSE?

We will only use your personal data for the stated purposes; unless we consider there to be a need to use it for another reason which is compatible with the original purpose.

If we consider it necessary and reasonable to use your personal data for an unrelated purpose, we will notify you and explain the legal basis which allows us to do so.

There may be circumstances where we have to process your personal data without your knowledge or consent, where this is required by law and in compliance with the above rules.

6. HOW DO WE USE YOUR SENSITIVE PERSONAL INFORMATION DATA?

We will only use your sensitive personal information (aka 'special category') data (further described at section 3) in the following ways:

- To comply with employment and other laws, e.g., when conducting right to work checks.
- Where required, when processing is in the public interest, e.g., for equal opportunity monitoring and reporting.
- To ensure we meet out health and safety obligations towards you, e.g., by assessing any disabilities you may have in order to make reasonable adjustments during the recruitment process (i.e., for interview purposes).
- To undertake criminal background checks, only as required by law, e.g., for safeguarding purposes and/or if the role requires a high degree of trust and integrity.

There may be circumstances where we need to process this type of information for legal claims or to protect your (or someone else's) interests and you are unable or capable of giving your consent or where the relevant

information has already been made public.

7. DO WE NEED YOUR CONSENT TO USE SENSITIVE PERSONAL DATA?

We do not need your written consent to use your 'special category' data, if it is used in accordance with this policy; to perform our legal obligations or exercise specific rights connected to your employment.

We may, in limited circumstances, need to request your written consent to process the special category data.

If written consent is required, we will provide you with details of the information we require and why we need it. You can then decide if you want to grant consent. Giving consent will always be a decision made by your freewill/choice.

8. WILL WE SHARE YOUR PERSONAL DATA WITH THIRD PARTIES?

To meet our legal obligations connected with your prospective employment/engagement it may be necessary to share your personal information with certain third parties (see below). We may also need to share your data when we have legitimate business reasons for doing so.

9. WHICH THIRD PARTY SERVICE PROVIDERS WILL WE SHARE YOUR PERSONAL DATA WITH?

The following third-party service provider may process personal information about you for the following purposes:

- Yoti Limited – to conduct digital right to work identity checks. Yoti are a UK Government verified IDSP.

We may also need to share your personal information with a regulator or to otherwise comply with applicable laws.

10. THIRD PARTY SERVICE PROVIDERS AND DATA SECURITY

Third party service providers can only process your personal data in accordance with our instructions. They must, in accordance with the Act, take appropriate measures to protect your privacy and personal information. We do not allow your information to be used by the third parties for their own purposes and business activities.

11. WILL WE TRANSFER YOUR PERSONAL DATA TO OTHERS AND/OR OUTSIDE OF THE UK/EEA?

The Company may from time to time need to make applicants personal information available to:

- other members of the Argonon Group, for the purposes set out in this Policy; or
- legal and regulatory authorities (such as HM Revenue and Customs or UK Visas and Immigration), to accountants, auditors, lawyers and other outside professional advisers, and to companies who provide products and services to the Company (such as IT systems suppliers, pension scheme, life assurance or medical benefit providers and intermediaries/brokers) and other third parties (collectively the "**Recipients**").

Although most Recipients will be in countries located within the European Economic Area ("**EEA**"), others may be located, or have relevant operations elsewhere. Therefore, it may be necessary for the Company to transfer your personal data to countries outside the EEA, in particular to the United States.

Some of these countries may not have laws regulating the use and transfer of personal data. In this case, the

Company will take steps to ensure that the Recipients whether internal or external, observe the principles set out in this Policy.

The transfer of personal data to third party service providers outside of the UK and the EEA will only take place on the basis of data protection adequacy decisions by the UK or the European Commission or via the implementation of EU data protection standard contractual clauses.

12. HOW DO WE ENSURE YOUR PERSONAL DATA IS SECURE?

We take your privacy and protection of data very seriously. Consequently, we have put in place appropriate security measures to prevent unauthorised use of your personal data.

Details of the measures which are in place can be obtained from the HR Department. We will notify you and any applicable regulator of any suspected unauthorised use of your personal data.

13. HOW LONG WILL WE KEEP YOUR PERSONAL DATA?

Unless we need to keep some of your personal information, following completion of the recruitment process (e.g., to comply with legal requirements), we will retain your information as follows:

- CVs – for a period of 3 years from completion of the recruitment process, for a particular role;
- Right to work check personal data – for a period of 7 years (in accordance with Employment and Immigration legislation and HMRC rules);
- Other information we collect as part of the recruitment process will be held until the end of the recruitment process.

If you are accepted for a role at our Company, the information collected during the recruitment process will form part of your ongoing personnel record and will be processed in accordance with our Employee, Freelancer & Talent Privacy Policy.

14. WHAT RIGHTS DO YOU HAVE IN RESPECT OF HOW WE USE YOUR PERSONAL DATA?

Subject to legal limitations you have the right to:

- **Request access to your data**: You can ask us to provide a copy of the personal data (and any supplementary information) we hold about you. Requests can be made verbally or in writing.
- **Request corrections to be made to your data**: If you think that your personal data is incomplete or inaccurate you can ask us to correct it – this will be dependent on the purposes of the processing.
- **Request erasure of your data**: If you consider there is no lawful basis for us to continue processing your data you can ask for that data to be deleted or removed.
- **Object to the processing of your data**: If our lawful basis for processing your data relates to a legitimate business interest (or third-party interest) you can raise an objection to that interest.
- **Request that processing restrictions be put in place:** If you believe that your information is being processed without a lawful reason or that the information is incorrect you can request that a freeze/restriction is placed on the processing of the information until your concerns are addressed.

When processing is restricted, we are allowed to continue storing the personal data, but cannot use it.

- **Request a transfer of your personal data**: You can ask us to transfer your personal data to a third party.

Please contact the HR Department if you want more information about how to exercise these rights.

15. WILL I HAVE TO PAY A FEE?

You will not be expected to pay a fee to obtain your personal data unless we consider that your request for access to data is unfounded or excessive. In these circumstances we may charge you a reasonable fee or refuse to comply with your request.

16. CONFIRMATION OF IDENTITY

When you make a request for access to your personal data, we may ask for specific information to confirm your identity. This is usually done to ensure that we are releasing personal data to the correct person.

17. RIGHT TO WITHDRAW YOUR CONSENT

If we have asked for your written consent to obtain information, you have the right to withdraw your consent at any time. To do so please contact our HR Department. Once we receive your notice of withdrawal, we will cease processing your data unless we have any other lawful basis on which to continue processing it.

18. UPDATES TO THIS PRIVACY POLICY

We reserve the right to amend or update this privacy policy from time to time in response to legal, technical or business developments. When we update this policy, we will take appropriate measures to inform you, which will be consistent with the significance of the changes we make.

If required by applicable data protection laws, we will obtain your consent for any material privacy policy changes.

19. HOW TO MAKE A COMPLAINT

To exercise all relevant rights, queries or complaints please (in the first instance) contact our Data Protection Manager (identified below at section 20).

If our Data Protection Manager is unable to resolve your complaint, to your satisfaction, you have the right to lodge a further complaint with the Information Commissioners Office on 03031231113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, England.

20. DATA PROTECTION TEAM

The following team will help Argonon fulfil the commitment's made in this policy statement.

Argonon Group:
Data Protection Manager(s) – Amanda Goddard / Makeda Evans (privacy@argonon.com)
HR and Office Administration Data Protection Lead – Jenny King
IT Data Protection Lead – Karl Dawkins
Finance Data Protection Lead – Chris Goulding

In addition, each company within the Argonon Group will identify a member of staff who will act as Data Protection Lead (with responsibility for the management and governance of data protection) for their company.

For any enquiries, please contact the Data Protection Manager(s).

21. RESPONSIBLE PERSON FOR POLICY

Overall responsibility for the Policy is:

Jenny King, Director of HR and Operations: Jenny.Korpalski@argonon.com

Key Nominated Senior Management:

Allison Todd, Managing Director of Windfall Films Ltd and key contact for Studio Leo Ltd
Henry Scott, Managing Director of Like A Shot Entertainment Ltd
Joey Attawia, Director of Leopard Pictures Ltd
Tom Porter, Creative Director of BriteSpark Films Ltd
Derek McLean, Managing Director of Bandicoot Productions Ltd and Bandicoot Scotland Ltd
Daniel Nettleton, Creative Director of Bandicoot Productions Ltd and Bandicoot Scotland Ltd
Steven McGovern, Chief Operating Officer of Argonon USA Ltd and Leopard USA Ltd
Joe Weinstock, Chief Executive Officer of Rose Rock Entertainment LLC

The following are Argonon departments and the current communication tree under this Policy:
1. CEO: James.Burstall@argonon.com
2. Director of HR and Operations: Jenny.Korpalski@argonon.com
3. Snr. Director of Technology: Karl.Dawkins@argonon.com
4. Global Director of Communications and Social Media: Rich.Turner@argonon.com
5. Head of Finance: Chris.Goulding@argonon.com
6. Chief of Legal and Commercial Affairs: Amanda.Goddard@argonon.com

Policy approved: 31st May 2023
Last update: 31st May 2023

Dated: 31st May 2023

Policy review procedure	
Responsibility	The Data Protection Manager(s) shall be responsible for reviewing this policy when legislative or industry updates are published, and in addition shall conduct a thorough review (in consultation with other members of the Data Protection Team (set out above)) in line with this procedure.
Procedure	The Data Protection Manager(s) shall meet to go through the current Policy, DP Breach Protocol, DP Crib Sheet & DPIA forms. These shall be reviewed, in consultation with other members of the Data Protection Team (set out above), and updated in terms of their effectiveness, their accurateness with current data protection law, updated technologies etc.
Timing	The review shall commence 3 months prior to the policy review date to be completed by the required date.
Review Completion Date	31st May 2024

For more information, please visit the ICO website: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/