Dated: 7th June 2026

ARGONON GROUP – DATA PROTECTION AND PRIVACY POLICY
(includes Employees, Freelancers, Crew, Talent & Contributors)

Dated: 7th June 2026

Dated: 7th June 2026

1. Introduction

The UK 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 gives individuals certain rights in relation to personal data that is held about them. This policy lets you know how we will fulfil our obligations under the Act to all who work within the Argonon Group or contribute to our programmes or other content.

The Argonon Group consists of Argonon Limited, and all subsidiary companies (collectively, "**the Company**", "**we**", "**our**" or "**us**"). Your employer is as named, in your contract of employment/engagement (with the address as set out in that contract), acting in its capacity as data controller.

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 employment/engagement relationship and post termination. This policy will explain 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 your employment/engagement, so that you are aware of how and why we are processing your personal data.

This policy applies to any employee or individual working for the Company in other capacities (such as freelancers, contractors, agency workers or any other individual performing a work activity or professional performance e.g., on-screen talent, for the benefit of the Company) collectively defined as "**you**", "**your**", "**your employment**" or "**your engagement**").

In addition, it also covers Contributors: Contributors are those people who appear in, are subjects of stories, or contribute to or apply to be part of, programmes or projects for development or broadcast, and podcasts, or any public exploitation, that are created for third parties. For example: applicants, contributors, participants and studio audience members, actors, presenters, hosts, podcasters, composers and musicians and other performers, talent, interviewees, witnesses etc, and their agents or other representatives, as well as people who appear in, are subjects of stories, or contribute to our, people or third parties who contact us with stories, queries, complaints, requests, feedback etc ("Contributors") as set out in Appendix 2.

We may update this policy at any time.

How to contact us?
If you have any questions about this Privacy Notice or how we use your personal information, please contact our Data Protection Manager privacy@argonon.com. See also section 26.
If you prefer, you can write to the DPO by post at:
Argonon Group,
1-3 S Peter's Street,
London,
N1 8JD

Please note that in respect of any Use of AI and Generative AI:
We sometimes use artificial intelligence to help us with production processes e.g. carrying out administrative tasks, creating costume models, transcribing scenes, compiling graphics, creating summaries, analysing stories etc. We don't always need your consent when we use AI. All our AI suppliers go through a due diligence process. Please see our Argonon AI Policy.

Dated: 7th June 2026

2. Data Protection Principles & Our Obligations To You

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

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

For certain programmes, particularly news, current affairs, and/or documentaries we may process your personal data for journalism, and archiving purposes, if in the public interest.

3. What Personal Data Will We Collect, Use And Store About You?

Prior to, or during the course of your employment/engagement, or involvement in a development or production with the Company, we may hold and process certain personal data which may also be required for the purposes of programme making and/or to comply with legal and regulatory obligations, for example Ofcom. Personal Data may be categorised as follows:
In some instances, if you do not provide this information we may not be able to continue with your request or we may not be able to continue to work with you or allow you to participate in programmes.

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

- Your name, salutation, addresses, contact numbers, and personal email addresses.
- Date of birth.
- Gender.

- Next of kin and emergency contact information.
- National Insurance number.
- Bank account details, payroll records and tax status information, tax authority information, including those that are based outside the UK and the EEA if you are subject to tax in another jurisdiction.
- Our professional advisers working on a matter which involves or is relevant to you.
- Salary, annual leave, pension and benefits information.
- Start date, and end date
- Passport and/or any other ID documentation.
- Location of employment or workplace.
- Copy of driving licence (only for individuals who drive for work).
- Recruitment and talent agencies information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process).
- Employment records (including job titles, work history, working hours, training records and professional memberships).
- Compliance with any data subject access requirements, including honouring any opt outs where applicable.
- Verification of identity and money laundering checks.
- Compensation history.
- Performance information.
- Disciplinary and grievance information.
- CCTV footage – in accordance with our CCTV Policy.
- Information about your use of our information and communications systems.
- Photographs.
- Compliance with Ofcom obligations.
- Our insurers, third party claims adjusters, insurance companies, and insurance regulatory authorities.
- Fraud prevention and detection organisations.
- Law enforcement agencies.
- Reporting for Silvermouse or and any deliverables requirement for the purposes of equality and diversity monitoring/reporting obligations.
- Governmental and competent regulatory authorities to whom we have regulatory applicable and necessary background and online checks from publicly available and accessible reports, directories and sources (such as Companies House and newspaper articles), social media platforms, and background search service providers.

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

- Information about your race or ethnicity, 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.
- Information about your trade union membership (if applicable) – we rarely process this information, when we do it is typically limited to certain roles that fall within the scripted production genre.
- Information about your health, including medical conditions, health and sickness records. Examples of when we would process information of this nature include obtaining medical reports to assess your eligibility for, or to administer and pay, benefits related to ill health (i.e., Company and statutory sick pay, private medical and life insurance). We may also use such data to assess or determine your fitness for employment, continued employment or a particular role or task, or to assess any risk to your health.
- 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. We will have the ability to access and export this data from the IDSP; storing it within our HR and payroll systems.
- Personal information when we research stories/complete our compliance obligations information about you (which may include sensitive information) from online searches, background check results about you, and/or other third parties (including for example informants, other individuals, or other companies/ organisations depending on the circumstances) when we research stories to report on; we want to understand more about a potential programme which may include you or your story, or we carry out our compliance obligations for Ofcom purposes.

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.

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.

4. How Do We Collect Your Personal Data?

We collect your personal data by a variety of means. We are likely to have collected some of the personal data outlined in section 3 above, during the recruitment and application process. This information may have been provided directly from you, an employment agency, background check provider and/or an IDSP. We may sometimes collect additional information from third parties including former employers and credit reference agencies.

During your time with us we may need to collect personal information outside of the categories identified in section 3. We will provide you with a written notice setting out the details of the purpose and the lawful basis

for collection of that additional data, its use, storage and your rights.

5. How Will We Use Your Personal Data?

The Company needs to collect and use personal data about employees for a variety of personnel, administration, employee, work and general business management purposes, which include:

- fulfilment of administrative functions such as HR, payroll, finance and business affairs;
- to fulfil our contractual obligations and make payment to you;
- the ability to monitor (as appropriate) use of our IT and communications systems, in accordance with current security policies and to ensure we can manage any disaster recovery requirements for the production or company if necessary and in adherence to any subject access requests or for the purposes of meeting any insurance or broadcaster requirements;
- the ability to carry out or co-operate with any complaints, disciplinary or investigation processes;
- the ability to monitor our premises using CCTV, for safety and security purposes;
- where reasonably necessary, the ability to obtain appropriate professional advice and insurance for the Company; and
- retention of data as necessary for compliance with operational needs and legal requirements, such as our compliance with obligations under Health and Safety legislation.

For the most part we will use your personal data for one of the following lawful bases:

- where we need to perform the contract we have with you.
- where we need to comply with a legal obligation.
- where it is necessary for our legitimate interests (or those of a third party). For example, to collect/process/store your personal data so that employee benefits you are entitled to can be administered correctly.
- Legitimate interests; Where we work with broadcasters there is a core legitimate interest in processing personal information for the purposes of broadcasting audio visual programming including for commercial exploitation and/or journalism. This includes “on-screen” and “off-screen” contributions from and about individuals. This is crucial to this activity and requires the processing of personal information.
- When we refer to a “programme” or a “production” in this privacy notice, we mean not just the finished programme, but also the broadcast, news items and features, rushes, clips, unused material and any other material or content we create including marketing, press, publicity, legal and/or commercial material.
- As part of fulfilling our core legitimate interest, we consider it necessary to process your personal information, so that we can: create commissioning proposals, materials and sizzles which may include your contribution; consider your application or your continuing involvement for a programme, ensuring we have the right talent, crew and contributors in our programmes; support, develop and maintain

journalism, individual and societal rights to receive information, and relevant and engaging programming and services; retain the programme and images including your contribution in our archive, for the purpose of monitoring or repeating the programme or otherwise using it for commercial purposes, our journalism or archiving in the public interest; (if applicable, provide to any third parties (e.g. travel agencies, resorts, hotels, transport providers - trains/taxis/airlines etc) who require your personal information to provide services during or as a result of your participation in a programme; seek advice from our professional advisors; share within the applicable broadcaster/commissioner to fulfil internal administration purposes; commercially make full use of the programme in the UK and around the world for the period in which we have rights in the programme, including the promotion and marketing of the programme.

- Please note: We also keep an archive copy after our rights have expired as a record of programming we have either made and/or broadcast; (i) in the event that we sell or buy any business or assets, we may disclose your information to the prospective seller or buyer of such business or assets, along with its professional advisors. In such circumstances the acquirer of the information will become the new data controller. We also have a legitimate interest to protect our business against fraud, breach of confidence, theft or proprietary materials, and other financial or business crimes. This means we have measures which include monitoring communications to/from us using our systems, protecting the security and integrity of our IT system.

It may also be necessary to process your personal data for other legal bases:

- To protect yours (or someone else's) vital interests, i.e., where processing might be necessary to protect someone's life; or prevent crime or fraud (unlawful acts).
- If required, in the public interest. For certain programmes, particularly news, current affairs, and/or documentaries we may process your personal data for journalism, and archiving purposes, in the public interest.
- Depending on the situation, there are also other legal conditions we sometimes rely on for example: obtaining legal advice and/or exercising our legal rights - sometimes we may need to keep and use your personal information to help us defend our legal position.
- Where you have made information publicly available we are allowed to use that information about you if it is reasonable for us to do so.

Exemptions

We may also rely on any exemptions available to us in order to process your personal information.

The law recognises that our work as a producer—particularly in news, documentary, investigative journalism, and creative programming—requires a balance between individual privacy and the public's right to be informed.

We sometimes rely on exemptions from certain data protection rules.

These allow us to protect confidential sources, maintain the integrity of ongoing investigations, or preserve the creative freedom necessary for our content.

We also apply exemptions where we are legally required to do so, such as for the prevention or detection of crime or to comply with regulatory requirements and/or court order.

This means that in specific scenarios, we may not be able to fulfil a request to access or delete your data if doing so would undermine these vital public interests or legal obligations. The most common exemptions we rely on are: the journalistic exemption or where we are assisting with the prevention or detection of crime, or where legal privilege or confidentiality rules apply.

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

6. When Will We Use Your Personal Data?

During your employment, and involvement with the production and for a period after the relationship has ended, we will use your personal information for specific purposes. The list below describes the purpose of our processing, the personal data involved (from section 3 above) and the lawful basis for our processing (from section 5 above):

- Determining the terms on which you work for us.
- Where the Company are working for broadcasters that are part of an industry-wide diversity monitoring initiative called Diamond, which is run alongside PACT, other UK broadcasters and the creative diversity network. Diamond uses personal information regarding on and off-screen contributors (which is anonymised) to programmes to report on the diversity of tv production in the UK.
- Where the Company is required to collect information for achieving access to Broadcaster's diversity commissioning spend, development for creatives from underrepresented groups.
- Where we keep records to create statistics and analysis in order to understand the effect impact of our own DEI initiatives and consider future initiatives.
- Checking your right to work in the UK.
- When making payments to you to also include any necessary statutory deductions.
- Providing employee benefits to you, which may include private medical insurance and life insurance.
- Liaising with your pension provider and ensuring payments are made.
- Administration related to the performance of your contract of employment/engagement.
- Business management and work force planning, including accounting and auditing.
- Conducting and managing reviews of performance and determining performance requirements.
- Making decisions regarding remuneration, bonus and/or commission.
- Making decisions regarding promotions to include assessing qualifications for a particular role.
- Gathering evidence for a possible disciplinary or gathering evidence in respect of any informal/formal complaint(s) or grievance(s).
- Making decisions about your continued employment or engagement.

- Making arrangements for the termination of our working relationship.
- Education, training and development requirements.
- Dealing with legal disputes involving you or other employees, workers and contractors, including accidents at work.
- Your information is shared with our employees and contractors working on the programme, supporting departments (for example finance or legal), and other companies within the group for purposes such as internal administration, storage, infrastructure, or programme production.
- We share data with those who make shows for us, and with external suppliers such as audience ticketing companies, providers assisting with diversity and inclusion initiatives, talent/recruitment agencies, after-show care providers, security services, and professional advisers (including lawyers, insurers, and auditors).
- Broadcasters and platforms: your information is shared with commissioning broadcasters and streaming platforms that buy or license our programmes for viewing; or receive publicity material for our programmes.
- Legal, regulatory and public interest bodies: this includes unions and industry representative bodies, law enforcement, government bodies, and regulators (such as Ofcom, the Information Commissioner's Office (ICO), the Jersey Office of the information Commissioner (JOIC), the Office of the Data Protection Authority (ODPA, in Guernsey). We may also be legally required to share your information due to a court order.
- Professional advisors: this includes external health and safety advisors, law firms, consultants etc who are able to provide any expert opinions or additional support we may require.
- Managing sickness absence, ascertaining your fitness to work.
- Complying with health and safety obligations, completion of accident book and RIDDOR reporting.
- CCTV monitoring for safety and security, and (where applicable) to use as supporting evidence for any disciplinary hearings. CCTV monitoring is always subject to our separate CCTV Policy.
- Monitoring use of our information and communication systems to ensure compliance with our internal procedures and prevention of security lapses and breach of data protection laws.
- Equal opportunities monitoring.
- Monitoring, and ensuring compliance with, the company's sustainability practices.

It's possible that some of the grounds for processing will overlap.

7. Your Responsibilities Under The Act

Your Personal Information

We will only ask you to provide information we believe is necessary for the performance of our employment/engagement relationship (e.g. using bank account details you provide to pay you) or our associated legal obligations (e.g. sharing your salary information with HMRC).

If you fail to provide certain information when requested, we may not be able to meet our contractual obligations to you or fulfil our legal obligations.

Other People's Personal Information

As well as having rights under the Act, you will also have a duty to comply with the data protection principles set out in section 2 (above).

You will be required to read, understand and accept any policies and procedures relating to personal data you may handle during your employment with, or engagement by, Argonon. This includes information: (i) provided during your induction; (ii) set out in your new starter form; (iii) set out in this policy; or (iv) contained within any other Company notices concerning data protection.

As part of your role, you may hold personal data about other Company employees or individuals (e.g. viewers, artists, contributors or business contacts) or be asked to disclose it by others. For example, if you have managerial responsibility for other employees, you are likely to hold personal data about them. Even if you do not have direct involvement with personal data as part of your job, there may be times when you are asked by others to supply personal data. Therefore, all employees must follow the guidelines set out below and in Appendix 1:

- All personal information must be kept securely and should remain confidential.
- If you receive a request from someone inside or outside the Company to give them any personal data about an employee (or other individual) you should follow the Employee Guidance Notes attached at Appendix 1. You should be aware that it is a criminal offence under the Act if you deliberately or recklessly disclose personal data to someone outside the Company without the Company's consent.
- Accessing, disclosing or otherwise using employee records or other employee personal data without authority will be treated as a serious disciplinary offence and may result in disciplinary action being taken in accordance with the Company's Disciplinary Rules and Procedure.
- You should not keep personal data about people which you no longer need or which is out of date or inaccurate. You should therefore review any personal data that you hold from time to time, bearing in mind the data protection principles set out at section 2.

Please note that the above applies to hard copy documents containing personal information, as well as information that is recorded and stored electronically.

8. 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 must process your personal data without your knowledge or consent, where required by law and in compliance with the above rules.

9. How Do We Use Your Sensitive Personal Information Data?

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

- To comply with employment and other laws, e.g. when conducting right to work checks at recruitment stage, when processing and managing situations connected with absences that arise in relation to your sickness, and/or family/dependant related leave.
- To ensure we meet our health and safety obligations towards you and other employment related obligations we will use information about your physical, mental health, or disability status to assess your capability to perform your role, monitor and manage your sickness absence, provide appropriate workplace adjustments and administer health related benefits.
- Where required, when processing is in the public interest, e.g. for equal opportunity monitoring and reporting.
- With your explicit consent.

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.

10. Do We Need Your Consent To Use Personal Data/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, e.g. before we can instruct a medical practitioner to prepare a medical report.

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. It is not a condition of your contract of employment or engagement that you must agree to any request for consent. Giving consent will always be a decision made by you, exercising your freewill/choice.

With respect to broadcast of a programme and if we need your consent, we must ensure we comply with the Ofcom Broadcasting Code and ensure there is a legal basis under data protection laws.

We do not generally rely on obtaining your consent to process your personal information for programmes being made by or for us.

11. Automated Decision Making

We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

12. Will We Share Your Personal Data With Third Parties?

To meet our legal obligations connected with your employment/engagement it may be necessary to share your

personal information with third parties (see below). We may also need to share your data when we have legitimate business reasons for doing so and where necessary, to perform your contract.

13. Which Third Party Service Providers Will We Share Your Personal Data With?

We work with a number of third-party service providers who process personal information about you for the following purposes:

- To provide and administer employee pensions;
- to issue and administer employee benefits (e.g. life assurance, EAP schemes, private medical insurance and administration of the Company's pension scheme);
- to fulfil the Company's HR administrative function via an online portal (hosted in the cloud);
- to conduct digital right to work identity checks e.g. finance or legal, and other companies like internal administration, storage, infrastructure, or programme production;
- broadcasters, platforms & distributors;
- legal, regulatory and public interest bodies;
- legal requirements to share your information due to a court order;
- health and safety;
- IT and cyber security;
- insurance requirements.

Please contact the Company Key Person, HR Department or Data Protection Manger(s) (noted below at section 25), if you want details of the companies currently providing the above services.

We may share your personal information with other third parties, for example, in the context of a possible sale or restructure of the business. We may also need to share your personal information with a regulator or to otherwise comply with applicable laws.

14. Third Party Service Providers And Data Security

Third party service providers can only process your personal data in accordance with our instructions and for the purposes set out in this Policy. 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 third parties for their own purposes and business activities.

15. 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 employee 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 such as any potential

purchasers of the company and broadcasters and distributors (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.

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.

16. 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. This is controlled and managed at Argonon by the Senior Director of IT who is based in the UK and in the US.

We will notify you and any applicable unauthorised use of your personal data.

17. How Long Will We Keep Your Personal Data?

We will retain your personal data for as long as is necessary to fulfil the purposes for which it was collected for.

The Company may, for example, keep details of employees for a reasonable time after they have left the Company. The Company needs to do this to ensure benefits have been properly administered, to give references (if requested to do so), to ensure that the Company's statutory/legal obligations (i.e., Tax, HMRC, Immigration) have been satisfied and to deal with any tribunal or other court proceedings.

We will generally retain personal data held within your personnel records for a period of 7 years following termination of employment/engagement, or for as long as required for investigations by authorised bodies. Following this period, your personal data will either be retained or securely destroyed, in accordance with applicable laws and regulations.

For contributors, Talent and Key Personnel linked to distribution, when we decide how long to keep your information, we think about how much personal information and the type of personal information we have, any risks to you if we use it, how important it is for us to use it and whether we can achieve our goals without using it, and other applicable legal or regulatory requirements. As general guidance, we may keep your contribution (for example, footage and recordings), contract details, payment records, participation records and publicity materials indefinitely for the ongoing use, airing and re-airing of the programme on any media, or archiving.

18. Your Duty To Inform Us Of Any Changes

To assist the Company in ensuring that your personal data is kept up to date and accurate, you should inform the HR Department of any changes to the following information:

- Address and other contact details;
- emergency contact name;
- bank account details;

- marital or civil partnership status.

In respect of Programmes, it enables us to ensure we keep you informed and enables us to comply with the 'Your Rights section as set out below.'

19. Your Rights

You have rights you can exercise over our use of your personal information. Some of these rights can only be exercised in certain circumstances and there may be exemptions that we can rely on. See information on exemptions.

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
- **Consent withdrawal**: where we have asked for your consent to use your personal information, you can withdraw that consent at any time. However, withdrawal may preclude or prevent you from your continuing participation in a programme. Consent to use your personal information under data protection law is different from informed consent obtained for the purposes of the Ofcom Code.
- **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. This right may be available when we automatically use your personal information on the legal basis of consent or performance of contract. However, it may not be technically possible and/or feasible for us to comply with your request). Please contact the HR Department if you want more information about how to exercise these rights.

Dated: 7th June 2026

20. Californian Residents

Californian residents have additional rights regarding their personal information under the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CCPR). As a Californian resident, in addition to the rights outlined in this notice, you can:

- **Request Disclosure**. You have the right to request disclosure of the categories and types of personal information we collect, use and share.
- **Request Deletion.** You have the right to request deletion of personal information we hold about you, subject to certain exceptions.
- **Request Corrections be made to your data.** You may request the correction of inaccurate personal information.
- **Request limitation of Use of Sensitive Personal Data.** You may restrict the processing of certain Sensitive Personal Data under certain circumstances. We will limit our use and sharing of Sensitive Personal Data only to those uses which are necessary to carry out our relationship with you, to fulfil our legal and regulatory obligations, to ensure the physical safety of you and others or as otherwise required under applicable privacy regulations;
- **Request right to Opt- Out of Sale or Sharing.** You have the right to opt out of any profiling or automated decision making, to the extent to which we engage in those processing activities.

To exercise your CCPA rights, please submit a request to:

Data Protection Manager privacy@argonon.com.
If you prefer, you can write to the DPO by post at:
Argonon Group,
1-3 S Peter's Street,
London,
N1 8JD

21. Australian Residents

Australian residents have additional rights regarding their personal information under the Australian Privacy Act 1988). As an Australian resident, in addition to the rights outlined in this notice, you can:

- **Request access to your data:** You can ask us to provide a copy of the personal data we hold about you. Requests can be made verbally or in writing.
- **Request corrections be made to your data:** If you think that your personal data is incomplete, inaccurate or outdated you can request correction.
- **Request right to anonymity and Pseudonymity:** Request to interact with us anonymously where possible.

- **Lodge complaints:** You have the right to lodge a complaint with the Office of the Australian Information Commissioner (OAIC) if you believe your personal data has not been correctly handled.

To exercise your Australian privacy rights, please submit a request to:

Data Protection Manager privacy@argonon.com.
If you prefer, you can write to the DPO by post at:
Argonon Group,
1-3 S Peter's Street,
London,
N1 8JD

More Information: Access your personal information | OAIC

22. 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.

23. 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.

24. Right To Withdraw Your Consent

If we have asked for your written consent to obtain information, you have the right (subject to the Act), to withdraw your consent at any time. To do so please contact your 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.

25. 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 to any material privacy policy changes.

26. How To Make A Complaint

The Data (Use and Access) Act 2025 requires every UK organisation which handles personal data to have a formal process in place allowing individuals to complain directly about how their personal data is handled, effective from 19th June 2026. Further information and guidance from the ICO can be found here.

To exercise all relevant rights, queries or complaints please (in the first instance) contact our Data Protection Manager (identified below at section 27).

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 0303 123 1113, via the live chat service or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, England.

27. Data Protection Team And Responsible Person For Policy

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

Data Protection Manager – Amanda Goddard (privacy@argonon.com)

Argonon Group:

HR and Office Administration Data Protection Lead – Jenny Korpalski
IT Data Protection Lead – Karl Dawkins
Finance Data Protection Lead – Matt Widmayer and Kyle Bergin

In addition, each Argonon Group company 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.

Key Nominated Senior Management and responsible for any subsidiaries or sister companies directly related to the parent company set out here.**:**
Allison Todd, Managing Director of **Windfall Films Ltd**
Henry Scott, Managing Director of **Like A Shot West Ltd**
Joey Attawia, Founding Director of **Leopard Pictures Ltd**
Tom Porter, Director of Programmes of **BriteSpark Films Ltd** and **BriteSpark Films East 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 Operations and HR: Jenny.Korpalski@argonon.com
3. Senior Director of Technology: Karl.Dawkins@argonon.com
4. Global Director of Communications & Social Media: Rich.Turner@argonon.com
5. Global CFO: Matt.Widmayer@argonon.com
6. Chief Legal and Commercial Officer: Amanda.Goddard@argonon.com

Policy approved: 07 June 2026
Renewal: 06 June 2027

Dated: 7th June 2026

Policy review procedure	
Responsibility	The Data Protection Manager shall be responsible for reviewing this policy when legislative or industry updates are published, and in addition shall conduct a thorough review in line with this procedure.
Procedure	The Data Protection Manager shall meet to go through the current Policy, and where applicable the DP Breach Protocol & 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 1months prior to the policy review date to be completed by the required date.
Review Completion Date	[xx November]

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

Dated: 7th June 2026

APPENDIX 1: Employee Guidance Notes

The rights of individuals impact the way in which you process data in certain key ways: (i) in collecting data; (ii) data security; (iii) deleting or destroying data; (iv) handling data requests; and (v) suspected breach of data.

i. Collecting Data

What do you need to tell individuals when you are collecting data?

At the point you obtain personal data about an individual, they should be informed of the following:

- the name and contact details of the organisation collecting the data;
- the purposes of the processing;
- the legitimate interests for the processing;
- whether individuals are under a statutory or contractual obligation to provide the data (if applicable);
- the recipients of the personal data, and whether that will require transfer of the data outside of the EEA;
- how long the data will be kept for;
- the rights available to individuals in respect of the processing;
- if applicable, the right to withdraw consent; and
- if required, the right to lodge a complaint with a supervisory authority.

Your Data Protection Lead (as notified to you on request by your manager) will inform you of how to communicate this when you are collecting personal data from an individual. If you are collecting special category or criminal offence data, please remember to seek explicit consent to the processing of such data.

In the event a contract is being issued to an individual, please ensure that it contains the up-to-date data protection clause as provided by the Data Protection Manager.

If you have obtained the personal data about an individual from a source other than the individual themselves, you should still inform them of the above information unless:

- the individual already has the information;
- providing the information to the individual would be impossible;
- providing the information to the individual would involve a disproportionate effort;
- providing the information to the individual would render impossible or seriously impair the achievement of the objectives of the processing;
- you are subject to an obligation of professional secrecy regulated by law that covers the personal data.

Be very clear with individuals about any unexpected or intrusive uses of personal data, such as combining information about them from a number of different sources.

If you have any questions regarding what to inform individuals about when collecting personal data, please ask your Data Protection Lead.

Please always bear in mind that the legitimate interest of processing the data must not be overridden by the rights or freedoms of the data subjects. Such risks to the rights and freedoms may include:

- processing which may give rise to discrimination, identity theft or fraud, financial loss, damage to reputation;
- where data subjects are prevented from exercising control over their personal data, e.g. right to access or remove;
- where personal data is processed which reveals racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures;
- where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; or
- where personal data of vulnerable natural persons, in particular of children, are processed. We treat any personal information about children and vulnerable people with the same care as any other personal information process. We recognise that children, in particular, merit specific protections with regards to their personal information. We may ask a parent/legal guardian/career for permission for some types of processing. Where children and/or vulnerable people are involved in the filming/production process, we ensure we follow strict Ofcom rules which may include additional safeguarding measures.

ii. Data Security

Data may only be used strictly for the purposes it was collected and should only be shared if necessary. If you have access to data that you do not need, then please notify your Data Protection Lead. You must be vigilant at all times as to security whilst on Argonon premises or elsewhere so that you do not access or disclose data without authority.

Premises

- The entrances to Argonon premises are manned by reception desks or require key codes to be entered to gain access. Doors must remain locked at all times if the reception desk is unmanned or if the key code lock is not in use. Do not leave fire doors ajar or jammed open.
- Visitors to Argonon's premises should be accompanied at all times.
- Argonon's premises are all equipped with alarms, security lighting and CCTV.
- Where possible, all computer screens and notice boards/white boards should be positioned away from windows/public view to prevent accidental disclosures of personal data. It is your responsibility to ensure that no visitors or guests to the office can view personal data.

Hard copy materials containing personal data

- No personal data should be written on notice boards/white boards situated around Argonon's offices unless it has been anonymised.

- Where possible, please operate a clean desk policy. This means that all hard copy materials, particularly those featuring personal data, are not left unattended on your desk.
- All paper waste containing personal data must be disposed in confidential waste bins situated at various locations around the office.
- Please be vigilant in relation to any hard copy materials containing copies of identification documentation (e.g. passports or driving licences), special category data, criminal offence data or personal data relating to children, which should be treated with the highest levels of security. Where possible, please scan all hard copy materials into a soft copy form for secure electronic filing and dispose of the hard copy materials as a matter of urgency. Where this is not possible, hard copy materials containing special category data, criminal offence data or personal data relating to children should be locked away in lockable drawers or cabinets at all times.
- Your Data Protection Lead will advise you on production specific guidance, however it is essential that you keep hard copy materials containing personal data to an absolute minimum. In the event, you need to take hard copy materials off the premises, please liaise with your Data Protection Lead as to how best to securely handle and store such materials. Never leave such materials laying in public view.
- A log of hard copy documentation containing personal data should be kept electronically to ensure its whereabouts and security is known at all times.
- On conclusion of a production, and unless otherwise agreed with the Data Protection Manager, the Data Protection Lead should ensure that all hard copy materials containing personal data are scanned and saved in secure electronic files before being confidentially destroyed, in order to minimise the risk of unauthorised access.

Electronic materials containing personal data

- All personal data should be stored in secure folders within Argonon's network. Data held within Argonon's systems are secured by file and folder level access protocols. Access to each file and folder must be granted via a system administrator.
- Access to personal data shall be granted on a "need to know" basis to individuals who are required to process it for the specific basis and purpose for which it was collected. Access to personal data is determined and monitored by the Data Protection Manager and the Data Protection Leads across Argonon.
- Electronic files and documentation containing personal data should be clearly labelled to ensure it can be located and accessed easily, if required.
- In the event, personal data is required to be accessed by multiple individuals, the Data Protection Leads should consider encrypting the files to ensure that they are 'read only' so as to ensure they are not altered or deleted incorrectly.
- Unless you have specific authority to process such personal data, you should not store such data on your desktop.

- Personal data may be stored electronically in many forms, and on a variety of devices – for example, USB sticks or camera memory cards. In the event, you need to send or take devices storing personal data off of Argonon's premises, please liaise with your Data Protection Lead as to how best to securely handle and store such devices.
- It is strictly prohibited to use your personal email accounts or non-Argonon systems to process personal data on behalf of Argonon. For the avoidance of doubt, this includes Google docs or document management systems that have not been approved by the IT Data Protection Lead. Please contact the IT Data Protection Lead for information and access to Argonon's secure document sharing platforms.

Security of electronic devices

- All Argonon computers are password protected. It is essential that you keep passwords secure and do not share accounts. Authorised users are responsible for the security of their passwords and accounts. User level passwords should be changed every 30 days. All computers must automatically lock after 15 minutes.
- All use of Argonon computers and Argonon systems, including all Argonon mailboxes, may be monitored or recorded to ensure compliance with Company policies or for security and/or legal reasons.
- Do not leave your computer or other electronic device unattended whilst unlocked.
- All other electronic devices should be secured with password protection. Information contained on portable devices is especially vulnerable, therefore special care should be exercised at all times.
- If you are issued with a work mobile we will ensure that they can be password locked and coded. At the end of your employment with the Company we will ask you to return all confidential and/or personal data or delete the information from any personal computer, tablet or mobile phone equipment you were using.
- All Argonon devices are protected by a secure firewall. You must exercise caution when opening unrecognised emails and attachments or visiting new websites to prevent viruses. All hosts used by the employee that are connected to the Argonon network, whether owned by the employee or Argonon, shall be continually executing approved virus-scanning software with a current virus database. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.
- If you take a laptop, hard-drives or other portable devices (e.g. USB memory sticks) off the premises you must make sure that the appropriate password protection and/or encryption is in place and that you have informed your Line Manager that you are taking data off site.
- If you are working at a location outside of Argonon's premises, please liaise with the IT Data Protection Lead as to how to ensure you are working in a manner which is technically secure.

iii. Deleting or Destroying Data

DO's:

- Delete or destroy any records that have passed their retention period – refer to our Record Retention Periods as notified by your Data Protection Lead.
- When you are disposing of paper files or documents containing personal information, you MUST always either shred them or discard them as confidential waste in the secure disposal bins located on your floor. These are the tall grey bins that have their lids sealed with locks.
- Delete documents and emails containing personal information off any device where they are no longer needed. For example, delete any contact lists (e.g. email contact lists) you no longer need.
- Set regular times for all files to be reviewed to see if anything can be archived, destroyed or deleted.
- If your employment/engagement with the Company ends (as a contractor or permanent employee), hand in all company-issued property (including laptops, tablets and work mobile phones) and delete any Argonon data off your personal devices (including work emails).

DON'T's:

- Hold onto documents or emails containing personal information when you no longer need that personal information. Delete or destroy unneeded personal information securely.
- Delete or destroy any legal documents (including releases) without consulting with your Line Manager. All legal documents should be kept for a minimum period of 7 years.

iv. Handling Data Requests

An individual can make a request verbally or in writing. It can be made to any part of our organisation (including by social media) and does not have to be a specific person or contact point. It just needs to be clear that they are asking for their own personal data.

You must ensure that you can identify when an individual has made a request to us. Having identified an individual's request, you must:

- immediately record the details of the request (particularly those made by phone or in person) detailing what the request is, why they want it and any relevant information pertaining to the collection and processing of the data that may be relevant to the request, including a list of recipients of the data; and
- where helpful, check with the requester that you have understood their request, as this can help avoid later disputes about how you have interpreted the request.

All requests must be acted upon without undue delay and at the latest within one month of receipt, therefore you should send such record immediately to your Data Protection Lead who will process the request with the Data Protection Manager. You may be required to assist with providing further information as required to process the request.

We also recommend that you keep a log of verbal requests.

Where an individual has made a subject access request, please note that it is an offence to make any amendment to personal data held by Argonon with the intention of preventing its disclosure.

v. Breaches of Personal Data

You have a responsibility to protect personal data – including the possibility that you may commit criminal offences if you deliberately try to access or disclose personal data without authority. If you have access to personal data, you shall not process that data unless we have instructed you to do so. It is vital that you understand the importance of protecting personal data and are familiar with the security policies and procedures outlined in this Policy.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data.

There will be a personal data breach whenever:

- someone accesses the data or passes it on without proper authorisation;
- the data is (maliciously or accidentally) corrupted, lost or destroyed; or
- if the data is made unavailable (e.g. encrypted by ransomware or lost).

For example, if you leave a USB stick containing personal data on public transport, or you send personal data to an incorrect recipient, a breach will have occurred.

If you are aware that a breach of personal data may have occurred, please notify your Data Protection Lead and the Data Protection Manager immediately as a matter of urgency.

In the event it is deemed necessary to report the breach to the Information Commissioner's Office, this must be done by us no later than 72 hours after becoming aware of the breach. It is therefore essential that you act quickly.

Additional Points to Note:

Data Protection Impact Assessments ("DPIA(s)")

Argonon recognises the need to carry out a DPIA in relation to processing that is likely to result in a high risk to individuals' interests. To assess the level of risk, both the likelihood and the severity of any impact on individuals should be considered. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

DPIAs should describe the nature, scope, context and purposes of the processing; assess necessity, proportionality and compliance measures; identify and assess risks to individuals; and identify any additional measures to mitigate those risks. It does not have to eradicate the risk but should help to minimise risks and consider whether or not they are justified.

DPIAs should consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm – whether physical, material or non-material – to individuals or to society at large.

Argonon has determined that DPIA(s) shall be completed, on a case-by-case basis (supported by the Data Protection Manager), when a company within the Argonon Group decides to use a new service (including technologies) and/or

commences a production that might (or have the potential to) process special category and criminal offence data, and such processing is likely to result in a high risk to individuals' interests.

DPIA(s) are live documents that should be updated regularly, considering for example, changes to a service being provided, or variations to data collection/processing during a production process.

Data Protection Officer (DPO)

Argonon recognises the requirement under legislation to appoint a DPO if:

- the organisation is a public authority; or
- if the organisation's core activities require large scale, regular and systematic monitoring of individuals (e.g. online behaviour tracking); or
- if the organisation's core activities require large scale processing of special categories of data or data relating to criminal convictions and offences.

Argonon Activities are the core activities of Argonon. Although Argonon processes special category and (on occasion) criminal offence data, it is not Argonon's core activity and it is not on a large scale, therefore Argonon has determined it does not need to appoint .

However, the Data Protection Manager (with support from the wider Data Protection Team, where applicable) have been appointed to assist Argonon in its compliance with this policy.

Transfers of personal data outside the EEA

Some of the people we share your personal data with are based outside of the UK. Personal data may only be transferred outside of the UK in compliance with the data protection principles set out in this Policy (at section 2).

Countries with adequacy decisions

Transfers may be made, without additional requirements, where the European Commission ("EC") has decided that a third country, a territory or one or more specific sectors in the third country, or an international organisation ensures an adequate level of protection.

As of the operational date of this policy the European Commission have made adequacy decisions on the following countries:

- Andorra;
- Argentina;
- Austria;
- Belgium;
- Bulgaria;
- Canada partial (in respect of data that is subject to Canada's Personal Information Protection and Electronic Documents Act only);
- Croatia;
- Cyprus;
- Czech Republic;
- Denmark;
- Estonia;
- Faroe Islands;

- Finland;
- France;
- Germany;
- Gibraltar;
- Greece;
- Guernsey;
- Hungary;
- Iceland;
- Isle of Man;
- Israel;
- Italy;
- Japan partial (in respect of private sector organisations only);
- Jersey;
- Latvia;
- Liechtenstein;
- Lithuania;
- Luxembourg;
- Malta;
- Netherlands;
- New Zealand;
- Norway;
- Poland;
- Portugal;
- Republic of Korea;
- Romania;
- Slovakia;
- Slovenia;
- Spain;
- Sweden;
- Switzerland;
- United States (Data Privacy Framework);
- Uruguay

The EC provides standard contractual clauses which offer sufficient safeguards on data protection for the data to be transferred internationally. Per the UK GDPR, companies can use an International Data Transfer Agreement (IDTA) and/or an International Data Transfer Addendum to provide the safeguards once covered by the EC's standard contractual clauses.

Further information can be found on the ICO website here

Transferring personal data to the US

In October 2023, the UK introduced a **US data bridge** in the form of a UK Extension to the EU-US Data Privacy Framework. The US data bridge allows the free flow of personal data from the UK to US based organisations that are appropriately certified under the scheme without the need for additional transfer mechanism or exception.

Further details can be found here
The US Data Privacy Framework List (which sets out all US certified companies) can be found here

Countries without appropriate decisions

With regards to countries where the EC have yet to make an adequacy decision, personal data may be transferred but only where the organisation receiving the personal data has provided adequate safeguards by means of: (a) the inclusion of standard data protection clauses that were included in contracts prior to the operational date of this policy continuing to be incorporated into all contracts; or (b) binding corporate rules (agreements governing transfers between organisations within Argonon's group companies).

This means that until such time that the EC provide further guidance on transfers to such countries, you may only transfer data where:

- protection provisions are included in contracts as provided by the Data Protection Manager; or
- intra-group within the Argonon group of companies.

We will continue to monitor the PACT and ICO websites and will update this policy if there are any further changes.

Dated: 7th June 2026

APPENDIX 2: Privacy Policy For Contributors

i. Introduction

The Data Protection Act 2018 and The Data (Use and Access) Act 2025 set out the principles that all companies within the Argonon Group must follow when processing personal data and gives individuals certain rights in relation to their personal data.

At Argonon, we are committed to keeping your personal data safe and secure. The Privacy Policy explains what personal data we collect, how we use it and what your rights are.

Personal information that you may give to us:

- If you're part of a news story: your name, contact details, your story and record of our discussions, interviews, footage (live or pre-recorded), any behind the scenes material, contributions, and anything you share with us on social media (like Instagram Stories, Instagram Live and other social media channels).
- We may also ask you about your more sensitive information such as physical or mental health, racial/ethnic origin, political opinions, trade union membership, sex life, sexual orientation, religion, philosophical beliefs, genetics, biometrics and/or information about your criminal offences (we will call all this "Sensitive Information") where it relates to the story or where we need to in order to meet our Ofcom obligations.
- Your correspondence with us where you write to us or otherwise send us information and anything else you send or tell us.
- Where you contact us to take part in a live programme (for example taking part in our live competitions/ phone-ins or where your name is announced as a winner on our live programmes).
- Personal information we may get from production companies.
- Information about you where you have provided the information as part of the production process, interviews, correspondence, information with friends, family members, and/or people connected to you where it relates to the programme or our Ofcom obligations;
- Sensitive Information where it relates to the programme, or a news story or where we need to know in order to meet our Ofcom obligations.
- Background and online check results about you from publicly available and accessible reports, directories and sources (such as Companies House and newspaper articles), social media platforms, and background search service providers. Personal information when we research stories/complete our compliance obligations.
- Information about you (which may include Sensitive Information) from online searches, background check results about you, and/or other third parties (including for example informants, other individuals, or other companies/organisations depending on the circumstances) when: we research

stories to report on; we want to understand more about a potential programme which may include you or your story, or we carry out our compliance obligations for Ofcom purposes.

We may also get contacted by third parties with information about you including:

- tax authorities, including those that are based outside the UK and the EEA if you are subject to tax in another jurisdiction;
- your bank or building society in connection with payments;
- our professional advisers working on a matter which involves or is relevant to you;
- governmental and competent regulatory authorities to whom we have regulatory obligations;
- audience ticketing companies and other broadcasters;
- recruitment / talent agencies;
- our insurer, and its representatives including brokers, third party claims adjusters, reinsurance companies and insurance regulatory authorities;
- fraud prevention and detection agencies and organisations;
- law enforcement agencies.

ii. Who are contributors?

This policy applies to any contributors, including:

- On screen talent (actors, writers, presenters, hosts, composers, musicians and other performers).
- People who are participants or apply to be in our TV programmes or in our studio audience (appear on a quiz show).
- Other people who contribute to our TV programmes (interviewees, people who send us videos and photos, people who let us use their property as a filming location).

This policy also applies to agents or other representatives of the contributors listed above.

iii. What personal data do we collect?

During pre-production, production and post-production, we may hold and process certain personal information. Depending on the programme you are involved in and the nature of your participation, we may collect:

- Your personal data in the application form, talent contract, consent form and correspondence about your contribution, including your name, email address, address, mobile phone number, date of birth, gender, residence status, nationality, pension number, financial details including bank account information, national insurance number.
- Your personal data as part of your contribution that identifies you (your image, voice, photos, property).

We may also collect **Special Category or Criminal Offence** personal data relating to your: race or ethnicity, political opinions, religious or philosophical beliefs, health, sex life or sexual orientation, genetics or biometrics, criminal offences, criminal convictions.

iv. How do we use your personal data?

We use your personal data for:

- **Contract performance:** when using your personal data to perform a contract with you.
- **Legal obligations:** when using your personal data is necessary for us to comply with applicable law.
- **Consent:** when you agree in advance that we can use your personal information in a specific way.

Where you are represented by a third party, we will share your personal data with your agent or representative.

v. How long do we keep your personal data for?

We will keep your personal data for as long as is necessary to fulfil the purposes for which it was collected for. We will generally retain personal data held within your personnel records for a period of 7 years following production. Following this period, your personal data will either be retained or securely destroyed, in accordance with applicable laws and regulations. If your contribution is not used in a programme, or is not intended for broadcast, we will delete your contribution much sooner, usually within 12 months of it being filmed or received by us.

vi. How do we ensure your personal data is secure?

We are committed to protecting your personal data and keeping it secure, private and confidential to prevent your data being lost, damaged, compromised, used or accessed unlawfully or without authorisation.

We put in place appropriate technical and organisational measures to help safeguard and protect your personal data, including providing training and guidance to production teams to ensure they understand how to keep your data secure.

vii. Children as contributors

If you are a parent or guardian of a child 13 years old or under and they are a contributor, please make sure that you explain to them what will happen to their personal data.

viii. Your rights

1. **Your right to request access to your data**: you can request a copy of records, files and documents containing your personal information.
2. **Your right to request corrections to be made to your data:** if you think your personal data is incomplete, inaccurate or not updated, you can ask us to correct it.
3. **Your right to request erasure of your data**: in specific circumstances, you can ask us to delete your personal information from our records.

ix. Handing Data Requests

Under **The Data (Use and Access) Act 2025**:

- If you are not satisfied with our use of your personal information, you are required to make a complaint to the company rather than going directly to the Information Commissioner's Office (ICO).
- Companies have 30 days to respond to the complaint and a 'stop the clock' rule allows companies to pause the response time if they need more information.

x. AI and data protection

The Data (Use and Access) Act 2025 provides greater flexibility for organisations to deploy AI systems, while enhancing protections for individuals:

Automated Decision Making: The Act eases existing restrictions on automated processing of personal data, giving organisations more scope to use AI-driven decision tools. Organisations must provide individuals with information about these decisions, enable them to challenge such decisions and allow them to request human intervention. The Act prohibits Automatic Decision Making in relation to special category data; this is only allowed with consent and requires strict safeguarding.

At Argonon, we do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

xi. Contacts

BBC:

- BBC Editorial Policy Section 7: Privacy
- Data Protection Corporate Policy (2025)
- BBC Records Management Corporate Policy (2025)

ITV:

- ITV Broadcasting Limited Privacy Notice for Contributors (2026)
- ITV Rights Limited Privacy Notice - Programme Applicants and Contributors (2026)
- ITV Producers Handbook (2024)
- Employee Privacy Notice (2023)

CHANNEL FOUR:

- Channel 4 Privacy Policy (2026)
- Channel 4 Contributor and Feedback Privacy Policy (2023)

OTHER:

- Ofcom Broadcast Standards: Privacy (2023)
- Producers' Data Protection and Security Guidelines (2018)

Dated: 7th June 2026

APPENDIX 3: Argonon Retention Policy

Please use as a template for Argonon Companies and insert the relevant Company details as required.

1. Contributors

The following applies unless the commissioning broadcaster requests a different retention period.

1.1. Applicants who apply to be on a specific programme, and are unsuccessful:

If they opt in for further communications:

Keep basic information (Name, email address, Gender, Address, Postcode, Home Tel, Mobile, Occupation, Photo) from their application form in order to contact about future castings and (insert relevant company) programmes and products, for six years or unless they contact us (i.e., through (insert relevant company e-mail)and/or privacy@argonon.com) and ask us not to.

Delete any other data (e.g. medical form/statement of health, criminal convictions self-declaration form, DBS check, notes of phone calls, release form) at end of production of that programme/series.

If they opt out from wanting to receive further communications:

Delete all information at the end of production of that programme/series or if, prior to completion of production, a contributor asks us not to delete such information we would retain it subject to their explicit consent. The personal data would then be collected, processed, and stored in accordance with the 'opt-in' process set out above.

1.2. Applicants who are successful:

Retain the following data which will be saved in Final Casting Paperwork folder for six years from time of creating application form or from the time needed to produce and exploit the programme – whichever time period is greater.

After the six-year period, review the position internally and decide whether we should retain the data for an extended period (i.e. if the programme is still being exploited).

Also use some judgement as to whether the programme had a sensitive nature to it and therefore it may be justifiable to keep documents such as psych reports for longer.

- PDF of application form
- Audition release form (if applicable)
- Personal disclosure form
- Statement of health
- Release form for show
- Signed Rules (if applicable)
- PDF Phone chat
- Background check (social media, Google and Lexis Nexis)
- Other including: Psych report, GP letters, DBS certificate, Prize winners letter / bank details form.

Dated: 7th June 2026

2. Employees and freelancers

Personal data collected, stored and/or processed as a part of the recruitment process will be subject to Argonon's Recruitment Privacy Policy located here and the below:

2.1. Speculative applications

If individuals send in speculative applications/CVs and there are no suitable positions available, (insert relevant company details)will retain data shared for a period of 24 months. Following expiration of this period the data will, with the exception of an applicant's contact information *[name, email, mobile, Last Position held)*, be deleted.

Speculative applicants can notify Bandicoot at any time and request that their data is deleted.

2.2. Advertised positions

CVs and completed application forms submitted for advertised positions shall be retained for a period of 3 years, from completion of the recruitment process.

2.3. Employees and freelancers

If an individual is accepted for a role at (insert relevant company details) (as an employee or freelancer), any information collected during the recruitment process will form part of their personnel record and processed in accordance with Argonon's Employee, Freelancer & Talent Privacy.

All data to be retained for the duration of the individual's employment/engagement plus 7 years. This includes any right to work check personal data.

Dated: 7th June 2026

APPENDIX 4: Data Breach Policy – Argonon Template

Please use as a template for Argonon Companies and insert the relevant Company details as required.

1. Introduction and scope

Personal data processed by, and on behalf of, (insert relevant company details) is subject to legislation that defines requirements to notify regulators (as well as the affected individuals) should a data breach occur. This policy spells out those requirements and the key actions that should be taken if an actual or suspected data breach occurs.

It covers all personal data processed by (insert relevant company details), its staff, freelancers (including those engaged via loan out companies) and by third parties on behalf of (insert relevant company details)..

2. What is a Data Breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data. For example, it includes the loss of a USB stick, data being destroyed or sent to the wrong email or postal address, the theft of a laptop or hacking.

Suspected breaches should be treated as an actual breach until it/they is/are proven not to be a breach to ensure that notification deadlines are not unduly delayed.

3. Internal Notification

Actual or suspected breaches should be reported immediately (and in any event within 24 hours) to *[please insert correct company contacts]* (Director of Production) via email and or phone. The data breach notification form attached at Appendix B should be completed and sent to *[please insert correct company contacts*] at the same time or, if this is not possible, as soon as possible thereafter.

If you have not had a response from any of the above people to your email or phone call within 12 hours then contact them again by phone.

Contact Details:

[please insert correct contact details]

4. Notifying individuals

Individuals whose data is subject to an actual breach should be notified by email without delay if the breach is likely to result in a high risk to their rights and freedoms. This should be done before notifying the regulator as it is a minimum expectation to minimise any potential harm.

The wording of the email MUST be approved by *[insert correct Company contact details]* who will consult with Argonon Legal and, if relevant to a specific programme, the commissioning editor of that programme. The email should include the following:

(i) An explanation of the breach;

(ii) Contact details of a person at (insert relevant company details) with whom the affected individual can raise any concerns or request further information;

(iii) An explanation of the likely consequences of the breach;

(iv) Details of measures taken or proposed to be taken to address the breach and, where appropriate, informing the individual of any measures taken to mitigate any possible adverse effects that may arise (or have arisen) as a result of the breach.

Do NOT notify individuals until Louisa has approved you doing so.

5. Notifying the regulator

[Insert correct Company contact details] along with Argonon Legal will conduct a breach impact assessment using the checklist at Appendix A to determine if the breach is notifiable to the Information Commissioner's Office (or relevant regulator outside the UK).

Deadline: 72 hours from internal notification.

Phone: 0303 123 1113 (open Monday to Friday, 9am to 5pm).

Web form located here (to be used if reporting outside of the above hours).

Post: Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

Notification Process: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/

If a breach is notifiable to the ICO the following information will be provided:

1) The nature of the personal data breach (i.e. confidentiality, integrity, availability);

2) The approximate number of individuals concerned and the category of individual (e.g. employees, mailing lists, service users);

3) The categories and approximate number of personal data records concerned;

4) The name and details of the person responsible for data protection at (Insert correct Company details)

5) A description of the likely consequences of the breach;

6) A description of the measures taken, or which we will take, to mitigate any possible adverse effects.

6. Records

[Insert correct Company details] is responsible for keeping a record of all personal data breaches, including those which the ICO are not required to be notified about.

Dated: 7th June 2026

APPENDIX 5: Data Breach Notification to ICO Checklist

Breaches should be notified to the ICO if they are likely to result in a high risk to the rights and freedoms of individuals.

'High Risk' means the threshold for informing individuals is higher than for notifying the ICO.

Consider the following:

1. What is the volume of data compromised?
2. What is the type of data compromised?
3. What is the actual harm to an individual as a result?
4. How was the data compromised?
5. What is the risk of it happening again without further action?
6. Where is the data processed that has been compromised?

Dated: 7th June 2026

APPENDIX 6: Data Breach Notification Form

Please use as a template for Argonon Companies and insert the relevant Company details as required.

Author of form and role at (Insert Company details)	
Name of production affected by breach (if any)	
Name of broadcaster affected by breach (if any) and name of relevant commissioning editor (if any)	
Date of incident	
Date when incident was discovered	
Detailed description of incident (i.e., provide a clear summary of what happen and when, and the steps that lead to the breach)	
Description of data affected. Is any of it sensitive in nature ('special category data')? Does it involve personal data relating to criminal convictions and offences or related to security measures? Special category data includes information about an individual's: • race; • ethnic origin; • politics; • religion;	

• trade union membership; • genetics; • biometrics (where used for ID purposes); • health; • sex life; or • sexual orientation.	
Number of individuals affected by breach (if known). How many data records are involved?	
Individuals involved in or aware of the breach and details of their involvement or awareness. Include internal and external individuals	
Action taken or proposed to be taken Examples of immediate action to take are: • change passwords; • shut down computers; • halt network traffic; or • restore data from backups.	
Details of measures currently in place that were intended to prevent such breaches. • What policies and procedures are in place? Are they written down? • What security measures are in place? Examples include: • Password protection; • Network security; or • Locks on doors and cabinets • Are staff trained in data protection policies and procedures, do you provide guidance for them to use as a reference?	

Dated: 7th June 2026

Ways of avoiding further similar incidents occurring in future What steps will be taken going forward, if any, to minimise the risk of such a breach occurring again in the future? This may include monitoring staff awareness of security issues and looking to fill any gaps through training or tailored advice.	
Other relevant information	