

BACK2BACK INTERNAL PRIVACY NOTICE

For employees, contractors, freelancers, interns, and other workers

Welcome to Back2Back's Internal Privacy Notice.

Back2Back respects your privacy and is committed to protecting your personal data. This privacy notice tells you about how we process your personal data and what your rights are.

1 Introduction

1.1 This privacy notice applies to any individual employed or engaged by Back2Back (or formerly employed or engaged by Back2Back) which includes employees, contractors, freelancers, interns and other workers ("**you**" and "**your**").

1.2 Please read this notice carefully. Among other things, it explains:

- **What personal data** we may collect about you in connection with: (i) your employment and/or engagement with us; and (ii) any related interaction between you and us;
- **How and why we process your personal data** and the lawful basis or bases by which we process your personal data together with other important information, such as how long we retain your personal data and who we share your personal data with; and
- **Your rights** in relation to the personal data we hold about you.

2 Who we are and our contact details

2.1 For the purposes of data protection laws, Back2Back Productions Limited ("Back2Back", "we", "us" or "our") is the data controller of your personal data which means that we are responsible for deciding how we hold and use your personal data.

2.2 If you have any questions about this privacy notice or the way we process your personal data, please contact us at:

Email address: becs.notman-watt@back2back.tv

Telephone: 01273 227700

3 What personal data we collect

3.1 The categories of personal data we may collect are included in the table below (depending on your role, certain categories of personal data listed below may not apply to you, particularly if you are not an employee):

Categories of Data	Description of Data
Identity Data	Name, address, date of birth, age, marital status and details of dependants, spouse and partner, title, maiden name, gender, nationality, country of residence, details of any disability information, sound recordings, images and/or photographs of you, driving licence, national ID card, passport and other identification and right to work documentation (including utility bills, national insurance number, social security number, tax number, residence permit, payslips or other), company/organisation name and details on a business card or in an email signature, hobbies, socio-demographic details.
Contact Data	Email address (work and personal), address, telephone number (work and personal), mobile number (work and personal), next of kin and emergency contact information and other information in an email signature.
Recruitment Data	Information contained in a Curriculum Vitae (“CV”) or cover letter, interview notes and feedback, references, details of background checks during your recruitment, copies of right to work documentation.
Employment Data	Employment contract/contract for services, start date, end date, location of employment or workplace, role, performance snapshots and review information, employment history (including job titles, work history, compensation history, working hours and professional memberships and professional qualifications), CV, education details, training details, disciplinary and grievance information, minutes or notes from a meeting, parental leave information, sickness records, details of any disability and medical information for any emergency situations, annual leave, pension and benefits information (medical and dental) and life assurance nominee details.
Financial Data	Bank account details, payroll records, tax and national insurance information, details regarding your financial position, assets, share options, income, salary and pay details.
Correspondence Data	Information which you provide in, or we learn about you from any correspondence or communications with us or our employees or our partners and advisors.
Usage Data	Device IP address, the pages of websites that you visit and searches made, information regarding your use of our information and communications systems (telephone, email, voicemail and internet) including date, time and duration and event logs (e.g. change in password) and contents of email messages and voicemail.

Security Data	Username, password, CCTV footage, footage from the live streaming of meetings and other information obtained through electronic means such as swipe card records and photographs.
Technical Data	Type of device, unique device identifier (e.g., an IMEI number, IP, or Mac address), network information, the type of operating system and browser you use, time zone settings and other device related information.
Publicly Available Data	Details obtained from online searches or that is otherwise available in public records including identity data, socio-demographic data and details obtained from LinkedIn, Facebook, Instagram or other social media networks.

3.2 We may process your special category data (also known as sensitive personal data) and data relating to Criminal Convictions and Offences in accordance with paragraph 4 below.

How we collect your personal data

3.3 We may collect personal data from you directly through your application and the recruitment process (e.g. through application forms and interviews, CVs and references), the onboarding procedure, through the administration of our benefits schemes, by completing forms, by corresponding with us by mail, phone, email or otherwise and generally through the course of job-related activities during the period of you working for us.

3.4 We may also obtain personal data from third parties or public sources including but not limited to the following:

- Employment agencies (if applicable);
- Former employers, business partners, referees and educational institutions;
- Our production partners;
- Service providers such as providers of HR, training, technical, payment and delivery services and providers of employment benefits;
- Government bodies such as relevant tax authorities;
- Public registers;
- Third party websites, such as LinkedIn, Facebook, Instagram or other social media networks; and

4 The purposes for which we process your personal data

4.1 We will only use your personal data when the law allows us to. Most commonly, we will process your personal data in any circumstances where such processing is necessary:

- For the performance of your employment/engagement contract (or another contract you have with us) or to take steps so we can enter into such contract with you;
- To comply with any legal obligation (for example to check your right to work); and/or



- For the purposes of the legitimate interests pursued by us or a third party and your interests and fundamental rights do not override those interests. These legitimate interests include the purposes identified in the table below but also include other commercial interests (including our interests in running a production company) and our internal administrative purposes.
- 4.2 Sometimes we may also process your personal data where we have your consent. Where we rely on consent as the lawful basis for processing your personal data, you have the right to withdraw your consent at any time.
- 4.3 On rare occasions, we may also need to process your personal data in the following circumstances:
- Where it is necessary to protect your vital interests or those of another person; and
 - Where it is necessary for the performance of a task carried out in the public interest such as equal opportunities monitoring.
- 4.4 We may process your personal data for more than one lawful ground depending on the specific purpose for which we are using your data.
- 4.5 We may process your personal data ourselves or in conjunction with our third-party service providers in accordance with paragraph 7 below.
- 4.6 Information about the purposes for which we use your personal data, the types of personal data we process to achieve these purposes, and the lawful basis by which we process it, is set out in the table below:

Purpose/Activity	Type of Personal Data Processed	Lawful Basis for Processing
<p>Recruitment</p> <ul style="list-style-type: none"> • Making a decision about your recruitment or engagement, the verification and assessment of your ability to work for or with Back2Back), to ensure that you are suitable for your role, interviewing you and obtaining references • To determine the terms on which you work with us • To carry out background checks and ensure you are legally entitled to work for or with Back2Back • To draft and enter into an employment/services contract with you • For administration purposes 	<ul style="list-style-type: none"> • Identity Data • Contact Data • Recruitment Data • Employment Data • Financial Data • Correspondence Data • Security Data • Publicly Available Data 	<ul style="list-style-type: none"> • Consent • Performance of a contract • Compliance with a legal obligation • Our legitimate interests and your legitimate interests: to operate and manage our business, recruit candidates who are able to perform the role, to maintain employment records and ensure good employment practice and comply with legal, regulatory and corporate governance obligations • Necessary for the establishment, exercise, or defence of legal claims • To carry out obligations and exercise rights in employment law • For reasons of substantial public interest (including equal opportunities monitoring)

Purpose/Activity	Type of Personal Data Processed	Lawful Basis for Processing
<p>Pay and Benefits</p> <ul style="list-style-type: none"> • To pay you and, if you are an employee, to deduct tax and national insurance contributions • To provide and administer Back2Back employee benefits including medical, dental, critical illness, pensions and insurances • To provide and administer share option and other incentive schemes (where relevant) 	<ul style="list-style-type: none"> • Identity Data • Contact Data • Employment Data • Financial Data • Correspondence Data 	<ul style="list-style-type: none"> • Consent • Performance of a contract including payment of salary, pay and employment related benefits • Compliance with a legal obligation • Our legitimate interests and your legitimate interests: to run and manage our business including to maintain employment records, ensure good employment practice, comply with legal and corporate governance obligations and to incentivise staff
<p>Employment/engagement lifecycle</p> <ul style="list-style-type: none"> • To update personal details including bank account details and benefits information • To carry out performance snapshots and assessments and assess qualifications for a particular job or task including decisions about promotions • To carry out salary reviews • To provide training • To gather evidence for possible grievance or disciplinary hearings and processes • To ascertain your fitness to work • To manage leave (including parental leave) and absence (including sickness absence) • To make decisions about your continued employment or engagement • To make arrangements for the termination of our working relationship • To provide references on request, either in respect to employment or a tenancy 	<ul style="list-style-type: none"> • Identity Data • Contact Data • Recruitment Data • Employment Data • Financial Data • Correspondence Data • Usage Data • Security Data • Technical Data • Publicly Available Data 	<ul style="list-style-type: none"> • Consent • Performance of a contract • Compliance with a legal obligation • Our legitimate interests and the legitimate interests of others: to ensure that you are suitable for the role, to run and manage our business including to record absences, maintain employment records, ensure safe working practices and good employment practice, to comply with legal and corporate governance obligations and to ensure our policies and practices are adhered to • Necessary for the establishment, exercise, or defence of legal claims • To carry out and exercise obligations and rights in employment law • For reasons of substantial public interest (including preventing or detecting unlawful acts, dishonesty and fraud and equal opportunities monitoring)

Purpose/Activity	Type of Personal Data Processed	Lawful Basis for Processing
<p>Business Management and Security</p> <ul style="list-style-type: none"> • To run and manage our business including the organisation of work, personnel management, secondments, accounting and auditing • To ensure the health, safety and welfare at work and comply with health and safety obligations • To provide appropriate workplace adjustments • To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems • To monitor use of our information and communication systems • To ensure the security of our, your and other's property • To prevent fraud • The sharing of your personal data with any prospective buyer or seller of any business or assets • To provide employee liability information under TUPE to the potential purchaser of a business • The processing of personal data in connection with any actual or prospective litigation or internal investigation 	<ul style="list-style-type: none"> • Identity Data • Contact Data • Employment Data • Financial Data • Correspondence Data • Usage Data • Security Data • Technical Data • Publicly Available Data 	<ul style="list-style-type: none"> • Consent • Performance of a contract • Compliance with a legal obligation • Our legitimate interests and the legitimate interests of others: to monitor and protect access to our network, systems and facilities, to run and manage our business including to maintain employment records, to ensure safe working practices and good employment practice, to comply with legal and corporate governance obligations and to ensure our policies and practices are adhered to and that commercially sensitive information is kept confidential • Necessary for the establishment, exercise, or defence of legal claims • To carry out obligations and exercise rights in employment law • For reasons of substantial public interest (including preventing or detecting unlawful acts, dishonesty and fraud)
<p>Analysis and monitoring</p> <ul style="list-style-type: none"> • To conduct data analytics studies to better understand employee hiring, retention and attrition rates 	<ul style="list-style-type: none"> • Identity Data • Contact Data • Recruitment Data • Employment Data • Correspondence Data 	<ul style="list-style-type: none"> • Consent • Performance of a contract • Compliance with a legal obligation • Our legitimate interests: to run and manage our business including, to maintain employment records, and

Purpose/Activity	Type of Personal Data Processed	Lawful Basis for Processing
<ul style="list-style-type: none"> To carry out equal opportunities monitoring To carry out surveys and obtain feedback 	<ul style="list-style-type: none"> Publicly Available Data 	<p>good employment practice, to comply with legal, regulatory and corporate governance obligations and to operate, develop and improve our business and ensure employee satisfaction</p> <ul style="list-style-type: none"> Necessary for the establishment, exercise, or defence of legal claims To carry out obligations and exercise rights in employment law For reasons of substantial public interest (e.g. equal opportunities monitoring)

4.7 We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal data for an unrelated purpose, we will notify you (which may be by way of an update to this notice) and we will explain the legal basis which allows us to do so.

4.8 Please note that we may process your personal data without your knowledge or consent where this is required or permitted by law.

How we use Special Category Data and Data relating to Criminal Offences or Convictions

4.9 We may process special categories of personal data (also known as sensitive personal data) including details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation and political opinions, and, information about your health (including any medical condition, disability, health and sickness records).

4.10 We will mostly only process your special category data where it is necessary for carrying out our rights and obligations under employment law or where we have your explicit consent to do so. Where we request your consent, we will provide you with full details of the personal data we wish to process and the reason for processing so that you can carefully consider if you wish to consent. You can withdraw your consent at any time. Please note that we may not always need your explicit consent to process your special category data and we may also process it where:

- You have made such personal data publicly known in a clear and obvious way;
- It is necessary for the performance of rights and obligations in the field of employment law;
- It is necessary to protect you or another person from harm;
- The processing is necessary for reasons of substantial public interest because of the law, such as equal opportunities monitoring or in relation to a pension scheme or to prevent or detect unlawful acts, dishonesty or fraud;



- The processing is necessary for the establishment, exercise, or defence of legal claims; and
- The processing is necessary for reasons of public interest in the area of public health.

4.11 We may in particular use your special category data in the following ways:

- We may use information about your physical or mental health or disability status (including any doctor's note or sick note) to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits including statutory maternity pay, statutory sick pay, pensions and health insurance (where relevant);
- We may use information relating to leaves of absence which may include sickness absence or family related leaves to comply with our legal obligations;
- We may use information about your gender, race, ethnic origin, age, or nationality to ensure meaningful equal opportunity monitoring and reporting; and
- To otherwise comply with our legal obligations.

4.12 We may also process information about criminal convictions and offences for the purposes of assessing your suitability for providing the services in respect of which you are employed or engaged (especially if the role involves working with children) and where the law allows and/or requires us to do so, including for reasons of substantial public interest (including the prevention or detection of unlawful acts, preventing fraud and protection the public against dishonesty).

5 What if you refuse to provide us with any personal data?

5.1 Where we need to collect personal data by law, or under the terms of a contract we have with you, and you fail to provide that data when requested, we may not be able to offer you employment, or properly perform the contract we have or are trying to enter into (such as paying you or providing a benefit), and this could affect the rights you would have under your contract.

6 Automated Decision Making

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

7 Sharing your personal data with third parties

7.1 We may share your personal data with third party suppliers who we engage to provide services which facilitate our business. We may share your business contact details (name, title, email address and telephone number) with such parties for pursuance of our legitimate interests or to perform contractual arrangements.

7.2 Details of third parties with whom we may share your personal data include (without limitation):

- Back2Back's production partners (including co-production companies, distributors and broadcasters), suppliers, promoters and advertisers ;

- Employment agencies, former employers, business partners, referees and educational institutions;
- Payroll providers, benefit providers to provide your pension;
- Healthcare and insurance providers;
- Training and compliance providers;
- IT providers such as cloud service providers, archive storage providers, and file sharing websites;
- Telephone providers, email providers, telephone and online conferencing services, and online training providers in order to set up accounts for you;
- Building security who maintain our access systems and CCTV systems;
- Our bank, insurance brokers, accountants, lawyers and other professional advisors;
- Relevant tax authorities.

7.3 We seek to ensure that any third party engaged by us who processes your personal data in connection with the purposes listed above has policies and procedures in place to ensure compliance with data protection laws.

7.4 For any third parties that are based, or process data, outside of the UK/EEA we engage such third parties in accordance with paragraph 8 below.

7.5 We may share your personal data with third parties where we are required to do so by law or regulation or in connection with other legal proceedings (including where we believe that your actions violate applicable laws or any agreement with us) or in order to protect our rights, property, or safety of our employees or others

7.6 In the event that our business or any part of it is sold or integrated with another business, your personal data may be disclosed to our advisers and those of any prospective purchaser and will be passed to the new owners of the business.

7.7 We may also disclose personal data to a third party where we are requested by you to provide a reference such as a reference to a new employer or a tenancy reference. We are not responsible for the actions of any third party that is not engaged by us and you should check their privacy practices and policies.

8 International data transfers

8.1 We may share your personal data with third-parties including external third-party service providers and production partners who may be based outside the UK and the EEA.

8.2 However, we will not transfer your personal data outside of the UK and the EEA unless:

- Such transfer is to a country or jurisdiction which the EU Commission and/or the UK has approved as having an adequate level of protection;
- Appropriate safeguards are in place in accordance with data protection laws. These safeguards include the use of standard contractual clauses or binding corporate rules; or
- The transfer is otherwise allowed under data protection laws (including where we have consent, the transfer is necessary for important reasons of public interest, is necessary for the establishment, exercise or defence of legal claims or is necessary for the performance of a contract with the data subject).

8.3 We will ensure that where your personal data is transferred outside of the UK and the EEA, it is afforded the same protection as would be afforded to it within the UK and the EEA.

9 **Data security**

9.1 We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality. We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

10 **Data retention**

11 As a minimum, we store your personal data for as long as your employment and/or engagement with us continues and then for up to 7 years after your employment and/or engagement ends, but for no longer than we need it including to fulfil our legal and regulatory obligations (e.g., relating to record keeping) and to exercise or defend any legal claims. See the Back2Back Data Retention Schedule for further detail.

12 **Your rights**

12.1 Under certain circumstances you have rights in relation to your personal data. See below a description of those rights:

- The right to request a copy of your personal data held by us;
- The right to correct any inaccurate or incomplete personal data held by us;
- The right to request that we erase personal data we hold about you;
- The right to request that we restrict the processing of your data;
- The right to have your personal data transferred to another organisation;
- The right to object to certain types of processing of your personal data by us; and
- The right to complain (please see paragraph 14 of this notice).

12.2 Please note that the above rights are not all absolute and are subject to applicable data protection law. If you wish to exercise any of the rights set out above, please contact us using the details provided above.

13 **Changes to the privacy notice and your duty to inform us of changes**

13.1 We may make changes to this notice from time to time, including as may be necessary or prudent to reflect any changes in the ways in which we process personal data or any changes in data protection laws. We will notify you of any substantive changes to this notice.

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

14 **Questions and Complaints**

14.1 We take our data protection obligations seriously. If you have any questions or complaints about this notice or the way that we handle your personal data, we would appreciate the chance



to deal with your concerns in the first instance before you approach the relevant data protection authority. Please contact us using the details provided in paragraph 2 above.

- 14.2 You have the right to make a complaint at any time to the relevant supervisory authority for data protection issues which, in the UK, is the Information Commissioner's Office (ICO) (www.ico.org.uk).

Last updated 21st August 2023