Unit 3, Clifton Mews, Clifton Hill, Brighton BN1 3HR

BACK2BACK PRODUCTIONS LTD

DATA PROTECTION POLICY

CONTENTS

1. Interpretation

1.1 Definitions:

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

Company name: **Back2back Productions Ltd**

Company Personnel: all employees, workers, contractors, agency workers, consultants, directors, members and others.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them.

Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for our own commercial purposes.

Criminal Convictions Data: means personal data relating to criminal convictions and offences and includes personal data relating to criminal allegations and proceedings.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programmes involving the Processing of Personal Data.

Data Processor: a natural or legal person which Processes Personal Data on our behalf (e.g. a supplier)

Data Protection Officer (DPO): the person required to be appointed in specific circumstances under the GDPR. Our DPO is Rebecca Notman-Watt

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

GDPR: the EU General Data Protection Regulation (*(EU) 2016/679*) and the same regulation as it forms part of the law of England and Wales.

Personal Data is subject to the legal safeguards specified in the GDPR.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories of Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy Guidelines: The Company privacy and GDPR related guidelines provided to assist in interpreting and implementing this Data Protection Policy and Related Policies, available from production@back2back.tv.

Privacy Notices (also referred to as Fair Processing Noticesor Privacy Policies): separate notices setting out information that may be provided to Data Subjects when the Company collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one-time privacy statements covering Processing related to a specific purpose.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Related Policies: The Company's policies, operating procedures or processes related to this Data Protection Policy (including the Information Security Policy attached) and designed to protect Personal Data, available from production@back2back.tv.

Special Categories of Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

2. Introduction

At Back2back Productions Ltd ("we", "our", "us", "the Company"), we collect and Process certain types of Personal Data in the course of business. Such Personal Data includes, for example, data about current, past and prospective employees and freelance staff, writers, directors, cast, contributors, contractors, and suppliers, and others with who we conduct business. It is vital that this information is Processed properly however it is collected, recorded or used.

This Data Protection Policy sets out some general principles that we adhere to at the Company. It also includes a schedule setting out the minimum appropriate time periods for which different types of data can be retained (the Data Retention Schedule) together with a policy setting out practical guidelines to ensure the security of the data which we Processes (Information Security Policy).

This Data Protection Policy applies to all Company Personnel ("you", "your"). You must read, understand and comply with this Data Protection Policy when Processing Personal Data on our behalf and attend training on its requirements. This Data Protection Policy sets out what we expect from you for the Company to comply with applicable law. Your compliance with this Data Protection Policy is mandatory. Related Policies and Privacy Guidelines are available to help you interpret and act in accordance with this Data Protection Policy. You must also comply with all such Related Policies and Privacy Guidelines. Any breach of this Data Protection Policy may result in disciplinary action.

Where you have a specific responsibility in connection with Processing such as capturing Consent, reporting a Personal Data Breach, conducting a DPIA as referenced in this Data Protection Policy or otherwise then you must comply with the Related Policies and Privacy Guidelines.

This Data Protection Policy (together with Related Policies and Privacy Guidelines) is an internal document and must not be shared with third parties, clients or regulators without prior authorisation from the DPO.

3. Scope

We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. The Company is exposed to potential fines of up to EUR20 million or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the GDPR.

All Company Directors and Managers are responsible for ensuring all Company Personnel comply with this Data Protection Policy and need to implement appropriate practices, processes, controls and training to ensure that compliance.

The DPO is responsible for overseeing this Data Protection Policy and, as applicable, developing Related Policies and Privacy Guidelines. That post is held by Rebecca Notman-Watt.

Please contact the DPO with any questions about the operation of this Data Protection Policy or the GDPR or if you have any concerns that this Data Protection Policy is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances:

(a) if you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by the Company) (see *paragraph 5.1*);

(b) if you need to rely on Consent and/or need to capture Explicit Consent (see *paragraph 6*);

(c) if you need to draft Privacy Notices (see *paragraph 7*);

(d) if you are unsure about the retention period for the Personal Data being Processed (see *paragraph 5.5 and the Data Retention Schedule attached*);

(e) if you are unsure about what security or other measures you need to implement to protect Personal Data (see *paragraph 5.5, 11 and the Information Security Policy attached*);

(f) if there has been a Personal Data Breach (*paragraph 12*);

(g) if you are unsure on what basis to transfer Personal Data outside the UK and EEA (see *paragraph 13.1*);

(h) if you need any assistance dealing with any rights invoked by a Data Subject (see *paragraph 14*);

(i) whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA (see *paragraph 18*) or plan to use Personal Data for purposes other than what it was collected for;

(j) if you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making (see *paragraph 19*);

(k) if you need help complying with applicable law when carrying out direct marketing activities (see *paragraph 20*); or

(l) if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors) (see *paragraph 13.2*).

4. Personal data protection principles

The Company and all Company Personal Processing Personal Data (and that is likely to be most personnel to some degree or other) must comply with the Personal Data protection principles summarised below. Personal Data must be:

(a) Processed lawfully, fairly and in a transparent manner (**Lawfulness, Fairness and Transparency**);

(b) collected only for specified, explicit and legitimate purposes (**Purpose Limitation**);

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (**Data Minimisation**);

(d) accurate and where necessary kept up to date (**Accuracy**);

(e) not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (**Storage Limitation**);

(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (**Security, Integrity and Confidentiality**); and

(g) Finally, we are responsible for and must be able to demonstrate compliance with the data protection principles listed above (**Accountability**).

5. Explanation of the data protection principles

5.1 Lawfulness, fairness and transparency

(a) Personal Data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject. This means that we will tell Data Subjects how we plan to Process their Personal Data (transparency), the Processing should match the description given to the Data Subject (fairness), and it must be for one of the purposes specified in the Data Protection Legislation (lawfulness).

(b) In general, 'transparency' and 'fairness' requires us to be clear and open with Data Subjects at the outset about how their Personal Data will be used, so that they can make an informed choice about whether they are happy for us to be Processing their Personal Data in this way. If anyone is deceived or misled when the information is obtained, then its use is unlikely to be fair. We will normally tell Data Subjects what Processing will occur by providing them with Privacy Notices. See the Privacy Notices (Notifying Data Subjects) section below for further detail.

(c) Processing will only be 'lawful' if one of the following requirements (or "lawful bases") are met:

i) **Consent:** the Data Subject has given consent to the Processing of their Personal Data for one or more specific purposes (more detail on what constitutes valid consent is included below).

ii) **Contract:** Processing is necessary for the performance of a contract with the Data Subject or in order to take steps at the request of the Data Subject prior to entering into a contract. Note that this only applies where there is a contract with the individual Data Subject (i.e.. not when we are contracting with a company).

iii) **Legal obligation:** Processing is necessary for compliance with a legal obligation to which we are subject.

iv) **Vital interests:** Processing is necessary in order to protect the vital interest of the Data Subject or of another natural person. This is likely to only apply in an emergency.

v) **Public function:** Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller. It is unlikely that this will apply to us.

vi) **Legitimate interests:** processing is necessary for the purposes of legitimate interests pursued by us or by a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject, in particular where the Data Subject is a child).

(d) For the Processing of Special Category Data and Criminal Convictions Data additional requirements must be met for such Processing to be considered lawful. See the Special Category Data and Criminal Convictions sections below for more information.

5.2 Purpose limitation

(a) Under the purpose limitation principle, personal Data shall be collected for specified, explicit and legitimate Purposes and not further Processed in a manner that is incompatible with those Purposes. This means that Personal Data must not be collected for one purpose and then used for another. For example, if we collect Personal Data from a person for the purposes of processing their application to be on one of our programmes, we should not then use their Personal Data to send them marketing material, without their express prior permission. If it becomes necessary to change the purpose for which the Personal Data is Processed, the Data Subject should be informed of the new purpose before any Processing occurs.

5.3 Data minimisation

(a) Under the data minimisation principle, Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purpose.

(b) This means that Personal Data should only be collected to the extent that it is required for the specific purpose notified to the Data Subject. Any Personal Data which is not necessary for that purpose should not be collected in the first place. What is necessary will vary depending on the reasons why the Personal Data is collected and what it is being used for. Company Personnel should always question what information is being collected and why.

(c) This also means that we must not store any Personal Data longer than strictly necessary. For more information, go to the Data Retention Schedule, which forms part of this policy.

5.4 Accuracy

(a) Under the Accuracy Principle, Personal Data should be accurate and kept up to date. Steps should therefore be taken to check the accuracy of any Personal Data at the point of collection and depending on the nature of the Personal Data, it should be checked at regular intervals to ensure it is up to date. Inaccurate or out of data should be destroyed.

5.5 Storage limitation

(a) Under the storage limitation principle, Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the Purposes for which the

Personal Data is processed. This means that we should, wherever possible, store Personal Data in a way that limits or prevents identification of the Data Subject. For more information, go to the Data Retention Schedule, which forms part of this policy

5.6 Security, integrity and confidentiality

(a) Under the security, integrity and confidentially principle, Personal Data shall be Processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful Processing, and against accidental loss, destruction or damage. This means that we must use appropriate technical and organisational measures to ensure the integrity and confidentiality of Personal Data is maintained at all times. For further information on how we seek to achieve this, please refer to the Information Security Policy attached, which forms part of this Data Protection Policy and to which all Company Personnel are required to adhere.

5.7 Accountability

(a) Under the accountability principle, we must be able to demonstrate that the six data protection principles listed above have been met. We do this through the provision of information in this policy, through providing clear information to our Data Subjects via Privacy Notices, keeping records of the data we keep and how it is Processed, through training Company Personnel and other practices and procedures. See paragraph 14 below (Accountability) for further details.

6. Consent

As described above, one of the 'lawful bases' for Processing Personal Data is to rely on the Data Subject's Consent. Under the GDPR, the threshold for obtaining valid Consent is very high. Consent is only one of the lawful bases for Processing Personal Data and is often not the most appropriate one to rely on.

A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to

Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

When processing Special Category Data or Criminal Convictions Data, we will usually rely on a legal basis for processing other than Explicit Consent or Consent if possible. Where Explicit Consent is relied on, you must issue a Privacy Notice to the Data Subject to capture Explicit Consent.

We must be able to evidence all Consents captured and keep records of all Consents in accordance with Related Policies and Privacy Guidelines so that the Company can demonstrate compliance with Consent requirements.

7. Privacy Notices (notifying Data Subjects)

The GDPR requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. The information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we must provide the Data Subject with all the information required by the GDPR including the identity of the Controller and DPO, how and why we will use, Process, disclose, protect and retain that Personal Data through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data.

When Personal Data is collected indirectly (for example, from a third party or publicly available source), we must provide the Data Subject with all the information required by the GDPR as soon as possible after collecting or receiving the data. We must also check that the Personal Data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

If you are collecting Personal Data from Data Subjects, directly or indirectly, then you must provide Data Subjects with a Privacy Notice in accordance with our Related Policies and Privacy Guidelines.

Please note that we have prepared the following Privacy Notices:

(a) **Website Privacy Notice**: this applies to anyone who visits our website.

(b) **Recruitment Privacy Notice**: this applies to anyone who applies to work for us.

(c) **Internal Privacy Notice**: this applies to any individual employed or engaged by us (or formerly employed or engaged by us) which includes employees, contractors, freelancers, interns and other workers.

(d) **Contributor and Talent Privacy Notice**: this applies to people who are applicants, participants, contributors, performers, presenters and audience members who may be featured in programmes or projects which a production brand of the Company intends to produce.

8. Special Category Data

We will only Process Special Category Data in accordance with the data protection principles set out above, and where the Data Subject explicitly Consents to such Processing, or where one of the following conditions applies:

(a) The Processing relates to Personal Data which has already clearly been made public by the Data Subject themselves.

(b) The Processing is necessary for the establishment, exercise or defence of legal claims.

(c) The Processing is specifically authorised or required by law (including employment law).

(d) The Processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically of legally incapable of giving Consent.

9. Criminal Convictions Data

We will only Process Criminal Convictions Data in accordance with the data protection principles set out above, and where the Data Subject expressly Consents to such Processing, or when such Processing is otherwise authorised by the GDPR. Where we Process Criminal

Convictions without the Data Subject's consent, it will usually be because it is necessary for the purposes of carrying out our legal obligations.

10. Children's Data

Children require particular protection when collecting and Processing their Personal Data, because they may be less aware of the risks involved (the age by which an individual is designated a child varies between 13 and 16 in accordance with national law. In the UK it is 13). It is our policy to obtain consent from a parent or guardian in relation to any person under the age of 18 applying to take part, being considered for or taking part in any of our programmes.

11. Information security

We will adopt physical, technical, and organisational measures to ensure the security of Personal Data. This includes the prevention of loss or damage, unauthorised alteration, access or Processing, and other risks to which it may be exposed by virtue of human action of the physical or natural environment. The Information Security Policy sets out the appropriate security measures to be adopted and procedures to be followed.

12. Reporting a Personal 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 unintended (e.g. losing a lap-top) and deliberate causes (e.g. our IT systems being hacked).

Any member of Company Personnel who knows of or suspects a Personal Data breach has occurred or may occur, must inform the DPO immediately. Examples of a potential breach would include where a Company Personnel member thinks that something they or one their colleagues has done or not done may have resulted in data being lost or compromised (e.g. losing a lap top or a memory stick or mobile device, or sending an email to the wrong person), or they believe that their computer may have been compromised by a virus, or anything else that they think is suspicious.

When a Personal Data Breach has occurred, we shall establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it is likely that there will be a risk then we will identify the Information Commissioner's Officer (ICO) without undue delay, but not later than 72 hours after becoming aware of it (which is why it is vital that the DPO is made aware of any Personal Data Breach immediately). If it is unlikely that there will be a risk, we may not report the breach to the ICO, but will document that decision and the reasons for it.

13. Sharing Personal Data and Data Transfers

Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share the Personal Data we hold with another employee, agent or representative of our group (which includes our subsidiaries and our ultimate holding company along with its subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions (see below for more detail on international data transfers).

You may only share the Personal Data we hold with third parties, such as our service providers, if:

(a) they have a need to know the information for the purposes of providing the contracted services;

(b) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

(c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

(d) the transfer complies with any applicable cross-border transfer restrictions; and

(e) a fully executed written contract that contains GDPR-approved third party clauses has been obtained.

13.1 International data transfers

The GDPR imposes restrictions on the transfer of Personal Data to countries outside of the UK and EEA (the EEA comprises the countries in the European Union and Iceland, Liechtenstein and Norway). These restrictions are in place to ensure that the level of protection of Data Subjects afforded by the Data Protection Legislation is not undermined when the data leaves the UK and EEA. We may transfer Personal Data to countries outside of the UK and EEA provided that one of the approved mechanisms under the Data Protection Legislation has been followed. Those mechanisms are as follows:

(a) The transfer is to a country or jurisdiction which the UK has approved as having an adequate level of protection. This currently includes all countries within the EEA, Gibraltar, Andorra, Argentina, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay.

(b) Appropriate safeguards are in place such as standard contractual clauses approved for use in the UK;

(c) The transfer is necessary for one of the other reasons set out in the UK GDPR including:

i) The performance of a contract between the Company and the Data Subject;
ii) Reasons of public interest;
iii) To establish, exercise or defend legal claims;
iv) To protection the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent; and
v) In some limited cases, for the Company's legitimate interests.

If you have any questions about your Personal Data being transferred to countries outside of the EEA, please contact the Data Protection Officer.

13.2 Transfers to third parties

We will generally only transfer Personal Data to, or allow access by, third parties when it is assured that the information will be Processed legitimately and protected appropriately by the recipient. Where third party Processing takes place, we will first identify if, under applicable law, the third party is considered a Data Controller or a Data Processor of the Personal Data being transferred.

Where the third party is deemed to be a Data Processor (they are a supplier for example), we will require the Data Processor under contract (i) to protect the Personal Data from further

disclosure and to only Process Personal Data in compliance with our instructions and (ii) to implement appropriate technical and organisational measures to protect the Personal Data as well as procedures for providing notification of Personal Data Breaches.

Where we are outsourcing services to a third party, we will identify whether the third party will Process Personal Data on its behalf and whether the outsourcing will entail any transfers of Personal Data to countries outside of the UK and EEA. Where necessary, it will include adequate provisions in the outsourcing agreement for such Processing.

14. Data Subject's rights and requests

Under certain circumstances, Data Subjects have rights when it comes to how we handle their Personal Data and can exercise their rights by making a Data Subject request These include the right to:

Be informed: Data Subjects have the right to be informed about the collection and use of their Personal Data. See the Privacy Notices (informing data subjects) section above for more information.

Access: Data Subjects have the right to access their Personal Data and other supplementary information via what is commonly known as a "Data Subject Access Request" or "DSAR".

Rectification: Data Subjects are entitled to have personal data rectified if it is inaccurate or incomplete.

Erasure: Data Subjects have the right to have their Personal Data deleted where there is no compelling reason for its continued Processing.

Restrict Processing: Depending on the circumstances, Data Subjects may have the right to block or suppress Processing of Personal Data. When Processing is restricted, we are permitted to store the Personal Data, but not further Process it. We can retain just enough information about the Data Subject to ensure that the restriction is respected in future.

Data Portability: This right enables individuals to obtain and reuse their Personal Data for their own purposes across different services. However, it only applies to Personal Data an individual has provided to us; where the Processing is based on that individual's consent or for the performance of a contract; and, when Processing is carried out by automated means. To the extent that Data Subjects are entitled to exercise this right, we must provide their

Personal Data in a commonly used, machine-readable format, and send it directly to another Data Controller if requested to do so by the Data Subject.

Right to Object: Data Subjects have the right to object to Processing e.g. for marketing purposes or where the lawful basis for processing is based on legitimate interests. To the extent that Data Subjects are entitled to exercise this right, we must stop Processing the relevant Personal Data unless we can demonstrate compelling legitimate grounds for the Processing, which override the interests, rights and freedoms of the individual; or, the Processing is for the establishment, exercise or defence of legal claims.

Not all these rights are absolute: in some circumstances they will not apply to the Data Subject concerned, or, to the particular use that we are making of their Personal Data.

When a Data Subject contacts us in order to exercise any of the rights referred to above, that is called a "Data Subject Request". There are no formalities for making a Data Subject Request - they can be made in writing or verbally, and the Data Subject does not need to use a specific form or words, refer to legislation, or direct the request to a specific contact.

We will be obliged to respond to a Data Subject Request without delay, and nearly always within a month at most. Given this, if a Data Subject Request is received by a Company Personnel member in respect of any of the above Data Subject rights listed above, they must contact the DPO immediately so that it can be dealt with appropriately. If a Company Personnel member receives a request from a Data Subject but they are unsure whether it is or is not a formal Data Subject Request, they should again contact the DPO immediately.

15. Accountability

15.1 We shall implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. We are responsible for, and must be able to demonstrate, compliance with the data protection principles.

We must have adequate resources and controls in place to ensure and to document GDPR compliance including:

(a) appointing a suitably qualified DPO (where necessary) and an executive accountable for data privacy;

(b) implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;

(c) integrating data protection into internal documents including this Data Protection Policy, Related Policies, Privacy Guidelines or Privacy Notices;

(d) regularly training Company Personnel on the GDPR, this Data Protection Policy, Related Policies and Privacy Guidelines and data protection matters including, for example, Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. The Company must maintain a record of training attendance by Company Personnel; and

(e) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

16. Record keeping

The GDPR requires us to keep full and accurate records of all our data Processing activities.

We must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents

These records should include, at a minimum, the name and contact details of the Controller and the DPO, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. To create the records, data maps should be created which should include the detail set out above together with appropriate data flows.

17. Training and audit

We are required to ensure all Company Personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

You must undergo all mandatory data privacy related training and ensure your team undergo similar mandatory training

You must regularly review all the systems and processes under your control to ensure they comply with this Data Protection Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

18. Privacy By Design and Data Protection Impact Assessment (DPIA)

We are under a general obligation to implement technical and organisational measures to show that it has considered and integrated data protection into all its Processing activities.

Therefore, when designing new systems or processes and/or when reviewing or expanding existing systems or processes, we shall endeavour to identify and address all data protection requirements and assess the impact of any new technology uses on the security of the Personal Data and, if appropriate, carry out a DPIA (see below). Wherever possible, encryption, pseudonymisation and anonymisation should be built into any new and/or revised systems or processes.

Any revised systems or processes will be approved by the DPO.

A DPIA is a process used to help identify and minimise the data protection risks of a project. We must carry out a DPIA for data processing that is likely to result in a high risk to individuals. The DPIA must:

(a) Describe the nature, scope, context and purposes of the processing;

(b) Assess necessity, proportionality, and compliance measures;

(c) Identify and assess risks to individuals by the processing; and

(d) Identify any additional measures to mitigate those risks.

To assess the level of risk when carrying out a DPIA, we must consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

Those conducting a DPIA should consult the DPO and, where appropriate, individuals and relevant experts.

19. Automated Processing (including profiling) and Automated Decision Making

Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

(a) a Data Subject has Explicitly Consented;

(b) the Processing is authorised by law; or

(c) the Processing is necessary for the performance of or entering into a contract.

If certain types of Special Categories of Personal Data or Criminal Convictions Data are being processed, then grounds (b) or (c) will not be allowed. However, the Special Categories of Personal Data and Criminal Convictions Data can be Processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

If a decision is to be based solely on Automated Processing (including profiling), then the Data Subject must be informed when you first communicate with them of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

We must also inform the Data Subject of the logic involved in the decision making or profiling, the significance and the envisaged consequences, and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

A DPIA must be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

20. Direct marketing

We are subject to certain rules and privacy laws when marketing to our customers.

For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt-in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

21. Changes to this Data Protection Policy

We keep this Data Protection Policy under regular review. This version was last updated on 21st August 2023 Historic versions can be obtained by contacting us

This Data Protection Policy does not override any applicable national data privacy laws and regulations in countries where the Company operates.

22. Acknowledgement of receipt and review

I acknowledge that I have received and read a copy of the Back2back's Data Protection Policy] and understand that I am responsible for knowing and abiding by its terms. I understand that the information in this Data Protection Policy is intended to help Company Personnel work

together effectively on assigned job responsibilities and assist in the use and protection of Personal Data. This Data Protection Policy does not set terms or conditions of employment or form part of an employment contract.

Signed …….

Printed Name …….

Date …….

BACK2BACK DATA RETENTION SCHEDULE

1 About this Schedule

1.1 This Data Retention Schedule includes minimum data retention periods for specific categories of documents. This is to ensure legal compliance (for example, with our data protection obligations) and accomplish other objectives, such as protecting intellectual property and controlling costs.

1.2 Company Personnel should comply with the retention periods listed in the Data Retention Schedule below. If you have any questions about this document please contact the Data Protection Officer.

1.3 This Data Retention Schedule was last updated on 23rd August 2023.

2 Corporate and Company Records

Type of Record	Retention Period	Reason/Comments
Accounting records.	3 years from the date they were made (private company)	Section 388(4) Companies Act 2006 (CA 2006) Tax requirements or other legislation may require longer.
Register of members.	Entries for former members can be removed 10 years after the date they ceased to be members.	Section 121, CA 2006
Register of directors.	Indefinite	Usual practice Section 162 of the CA 2006 requires the register to be kept but legislation is not explicit about retention periods. General practice is to retain details of current and former directors, together with date of ceasing to be a director.
Register of directors' residential addresses.	Remove addresses of former directors after [6] years.	Best practice Section 165 of the CA 2006 requires the register to be kept but there is no statutory retention period or indication whether addresses of former directors should be removed.
Health and safety inspections, property management and asset records.	6 years	Health and Safety at Work Act 1974 and Limitation Act 1980 (LA 1980)

3 Facilities and Security Records

Type of Record	Retention Period	Reason/Comments
CCTV recordings.	*[90 days for routine recordings]*	Best practice No set period in law but as these can contain personal data, should be kept for no longer than is necessary for the purpose.
Visitor logs.	6 months	Best practice No set period in law but as these can contain personal data, should be kept for no longer than is necessary for the purpose.

4 Legal Records

Type of Record	Retention Period	Reason/Comments
Legal advice and opinions (non-litigation).	7 years after life of the matter the advice relates to	Business need
Legal advice and other records relating to specific litigation or claim.	7 years from settlement or withdrawal of claim	Limitation period + 1 year
Data subject rights requests	7 years from closure of request	Limitation period + 1 year
Previous versions of policies, including IT policy, privacy policy, retention policy etc.	7 years form being superseded	Business need and limitation period + 1 year in the event of a related claim
Monitoring and investigation requests	7 years from closure of investigation	Limitation period + 1 year
Insurance claims	7 years after settlement	Limitation period + 1 year

5. **Employment and HR Records**

Type of employment record	**Retention period**
Recruitment records These may include: Completed online application forms or CVs. Equal opportunities monitoring forms. Assessment exercises or tests. Notes from interviews and short-listing exercises. Pre-employment verification of details provided by the successful candidate. For example, checking qualifications and taking up references. (These may be transferred to a successful candidate's employment file.) Criminal records checks. (These may be transferred to a successful candidate's employment file if they are relevant to the ongoing relationship.)	Six months after notifying candidates of the outcome of the recruitment exercise.
Immigration checks	Three years after the termination of employment.
Contracts	
These may include: Written particulars of employment. Contracts of employment or other contracts. Documented changes to terms and conditions.	While employment continues and for seven years after the contract ends.
Collective agreements	
Collective workforce agreements and past agreements that could affect present employees.	Any copy of a relevant collective agreement retained on an employee's record will remain while employment continues and for seven years after employment ends.
Payroll and wage records	
Payroll and wage records Details on overtime. Bonuses. Expenses. Benefits in kind.	These must be kept for at least three years after the end of the tax year to which they relate. However, given their potential relevance to pay disputes they will be retained for seven years after employment ends.

Current bank details	Bank details will be deleted as soon after the end of employment as possible once final payments have been made
PAYE records	These must be kept for at least three years after the end of the tax year to which they relate. However, given their potential relevance to pay disputes they will be retained for seven years after employment ends.
Payroll and wage records for companies	These must be kept for six years from the financial year-end in which payments were made. However, given their potential relevance to pay disputes they will be retained for seven years after employment ends.
Payroll and wage records for unincorporated businesses	These must be kept for five years after 31 January following the year of assessment. However, given their potential relevance to pay disputes they will be retained for seven years after employment ends.
Records in relation to hours worked and payments made to workers	These must be kept for three years beginning with the day on which the pay reference period immediately following that to which they relate ends. However, given their potential relevance to pay disputes they will be retained for seven years after the working relationship ends.
Travel and subsistence.	While employment continues and for seven years after employment ends.
Record of advances for season tickets and loans to employees	While employment continues and for seven years after employment ends.
Personnel records	
These include: Qualifications/references. Consents for the processing of special categories of personal data. Annual leave records. Annual assessment reports. Disciplinary procedures.	While employment continues and for seven years after employment ends.

Grievance procedures. Death benefit nomination and revocation forms. Resignation, termination and retirement.	
Records in connection with working time	
Working time opt-out	Three years from the date on which they were entered into.
Records to show compliance, including: Time sheets for opted-out workers. Health assessment records for night workers.	Three years after the relevant period.
Maternity records	
These include: Maternity payments. Dates of maternity leave. Period without maternity payment. Maternity certificates showing the expected week of confinement.	Four years after the end of the tax year in which the maternity pay period ends.
Accident records	
These are created regarding any reportable accident, death or injury in connection with work.	For at least four years from the date the report was made.
Pension records	
These include: Pension admin Pension records (including pension contribution forms)	12 years from the end of any benefit payment under the policy.

6. **Production records**

Type of record	**Retention Period**
All Production documents, including but not limited to; Production Contracts Call Sheets Release Forms Background Checks Duty Of Care checks Rushes Master Programmes	Duration of the term, as specified by the broadcaster. Please check with your Production Manager for details. The licence term is usually between

Stills Contact details/ casting database Unit Lists	

BACK2BACK INFORMATION SECURITY POLICY

1 **About this policy**

1.1 Our IT and communications systems are intended to promote effective communication and working practices. This policy outlines the standards you must observe when using these systems, when we will monitor their use, and the action we will take if you breach these standards.

1.2 The Data Protection Officer has overall responsibility for this policy, including keeping it under review.

1.3 In serious cases, breach of this policy may be treated as gross misconduct leading to summary dismissal.

1.4 This policy does not form part of any employee's contract of employment and we may amend it at any time.

1.5 This Information Security Policy was last updated on 21st August 2023

7. **Equipment security and passwords**

(a) You are responsible for the security of the equipment allocated to or used by you, and you must not allow it to be used by anyone other than in accordance with this policy. You should use passwords on all IT equipment, particularly items that you take out of the office. You should keep your passwords confidential and change them regularly.

(b) You must only log on to our systems using your own username and password. You must not use another person's username and password or allow anyone else to log on using your username and password.

(c) If you are away from your desk you should log out or lock your computer. You must log out and shut down your computer at the end of each working day.

8. **Systems and data security**

(a) You should not delete, destroy or modify existing systems, programs, information or data (except as authorised in the proper performance of your duties).

(b) You must not download or install software from external sources without authorisation from the Data Protection Officer. Downloading unauthorised software may interfere with our systems and may introduce viruses or other malware.

(c) You must not attach any device or equipment including mobile phones, tablet computers or USB storage devices to our systems without authorisation from the Data Protection Officer.

(d) We monitor all emails passing through our system for viruses. You should exercise particular caution when opening unsolicited emails from unknown sources. If an email looks suspicious do not reply to it, open any attachments or click any links in it.

(e) Inform the Data Protection Officer immediately if you suspect your computer may have a virus.

(f) Confidential information must not be removed from the Company's offices without permission from the Data Protection Officer except where that removal is temporary and necessary (e.g. in accordance with the Working from Home provisions set out below).

9. **Working from Home**

(a) Confidential or other information should only be taken to your home if you have appropriate technical and practical measures in place to maintain the continued security and confidentiality of that information.

(b) No confidential information is to be stored on your home computer (PC, laptop or tablet).

(c) Documents should not be printed at home unless absolutely necessary. Leaving hard copy documents around your home could result in a personal data breach if they are accessed by a third party together with client confidentiality and other regulatory issues. As such, files and confidential information must be kept in a secure environment where they cannot be accessed by family members or visitors and then disposed of securely.

10. **IT System Management**

(a) Our IT systems are managed by suitably trained staff who are responsible for overseeing day-to-day operation and to ensure continued security and integrity.

(b) Access controls will be maintained at appropriate levels for all systems by ongoing and proactive management. Any changes to permissions must be approved by the Data Protection Officer.

(c) New IT systems, or upgrades to existing systems, must be authorised by the Data Protection Officer and the authorisation process must take account of security requirements. The information assets associated with any proposed new or updated systems must be identified and a risk assessment undertaken.

(d) Any new equipment must have appropriate levels of resilience and fault tolerance and must be correctly maintained.

(e) Software and applications must be managed to ensure their smooth day-to-day running and to preserve data security and integrity. The purchase or installation of new or upgraded software must be planned and managed and any information security risks must be mitigated. Specifications for new software or upgrades of existing software must specify the required information security controls.