



DATA PROTECTION POLICY

Policy Statement

Every day our business receives, uses and stores personal information about our colleagues and everyone else with whom we deal during the course of our working day (regardless of whether or not they are EU citizens or residents). It is important that this information is handled lawfully and appropriately in line with the requirements of the General Data Protection Regulation (in force 25 May 2018), any resulting enactment and any amendments or revisions thereto, under the laws of England and Wales (collectively referred to as the "Data Protection Requirements").

We take our data protection duties seriously because we respect the trust that is being placed in us to use personal information appropriately and responsibly.

About This Policy

This policy covers all individuals working for M R Production World Tour Ltd ("MRWT") (the "Company", "our", "us" or "we") (unless you are notified otherwise) at all levels and grades, and in any role, whether in management or production, including senior managers, officers, directors, employees, consultants, contractors, freelancers, trainees, interns, home-workers, interns, part-time and fixed-term employees, casual and agency staff and volunteers (collectively referred to as "staff").

This policy, and any other documents referred to in it, sets out the basis upon which we will process any personal data we collect.

This policy does not form part of any contract of employment or contract for services and may be amended at any time.

PendaBede Stally is responsible for ensuring compliance with the Data Protection Requirements and with this policy and shall be referred to as the "Data Protection Compliance Manager". Any questions about the operation of this policy and any document to which it refers, or any concerns that the policy has not been followed, should be referred in the first instance to the Data Protection Compliance Manager (email c/o dataprotection@ngm.global).

What is Personal Data?

Personal data means data (whether paper-based or digital) relating to a living individual who can be identified directly or indirectly from that data (or from that data and other information in our possession).

Processing is any activity that involves use of personal data. It includes obtaining, recording or holding the data, organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Special category personal data includes personal data about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic, biometric, physical or mental health condition, sexual orientation or sexual life (what used to be known as "sensitive personal data"). It can also include data about criminal offences or convictions. Special category personal data can only be processed under strict conditions, including with the consent of the individual.

Data Protection Principles

Anyone processing personal data must ensure that data is:

- a) processed fairly, lawfully and in a transparent manner;
- b) collected for specified, explicit and legitimate purposes and any further processing is completed for a compatible purpose;
- c) adequate, relevant and limited to what is necessary for the intended purposes;
- d) accurate, and where necessary, kept up to date;
- e) kept in a form which permits identification for no longer than necessary for the intended purposes;
- f) processed in line with the individual's rights and 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, using appropriate technical or organisational measures;
- g) not transferred to people or organisations situated in countries without adequate protection and without firstly having advised the individual.

Fair and Lawful Processing

The Data Protection Requirements are not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the individual. In accordance with the Data Protection Requirements, we will only process personal data where it is required for a lawful purpose. The lawful purposes include (amongst others): whether the individual has given their consent, the processing is necessary for performing a contract with the individual, for compliance with a legal obligation, or for the legitimate interest of our business. When special category personal data is being processed, additional conditions must be met.

Processing for Limited Purposes

In the course of our business, we may collect and process the personal data set out in our Staff Privacy Notice (and any other privacy notices that we may deem necessary from time to time). This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, location data, business partners, agents, fixers, sub-contractors and others). We will only process personal data for the specific purposes set out in our Privacy Notices or for any other purposes specifically permitted by the Data Protection Requirements. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

Notifying Individuals

To the extent required by the Data Protection Requirements, if we collect personal data directly from an individual, we will inform them about:

- a) the purpose or purposes for which we intend to process that personal data, as well as the legal basis for the processing;
- b) where we rely upon the legitimate interests of the business to process personal data, the legitimate interests pursued;
- c) the types of third parties, if any, with which we will share or disclose that personal data;
- d) the fact that the business intends to transfer personal data to a non-EEA country or international organisation and the appropriate and suitable safeguards in place;
- e) how individuals can limit our use and disclosure of their personal data;
- f) information about the period that their information will be stored, or the criteria used to determine that period;
- g) their right to request from us, as the controller, access to and rectification or erasure of personal data or restriction of processing;

- h) their right to object to processing and their right to data portability;
- i) their right to withdraw their consent at any time (if consent was given) without affecting the lawfulness of the processing before the consent was withdrawn;
- j) the right to lodge a complaint with the Information Commissioner's Office;
- k) other sources where personal data regarding the individual originated from and whether it came from publicly accessible sources;
- l) whether the provision of the personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the individual is obliged to provide the personal data and any consequences of failure to provide the data;
- m) the existence or otherwise of any automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the individual.

If we receive personal data about an individual from other sources, e.g. artists' agents or orchestral fixers, we will provide them with this information as soon as practicably possible (in addition to telling them about the categories of personal data concerned). At the time of writing, we do not anticipate receiving personal data about an individual from any kind of third-party marketing or promotions business but if we do, we will amend this policy accordingly.

We will also inform data subjects whose personal data we process that we are the data controller with regard to that data, what our contact details are (c/o Nick Grace Management, 20 Petersham Road, Richmond, TW10 6UR; dataprotection@ngm.global) and who the Data Protection Compliance Manager is.

Adequate, Relevant and Non-Excessive Processing

We will only collect personal data to the extent that it is required for the specific purposes notified to the data subject.

Accurate Data

We will ensure that personal data we hold is accurate and kept up-to-date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

Timely Processing

We will not keep personal data longer than is necessary for the purpose or purposes for which it was collected.

Accordingly, we have a General Data Retention Policy in place. We also have contractual arrangements with our data processors which require them to abide by the relevant Data Protection Requirements.

Processing in line with Data Subjects' Rights

We will process all personal data in line with data subjects' rights, in particular their right to:

- a) confirmation as to whether or not personal data concerning the individual is being processed;
- b) request access to any data held about them by a data controller (see also Clause 14 Subject Access Requests);
- c) request rectification, erasure or restriction on processing of their personal data;
- d) lodge a complaint with a supervisory authority;
- e) data portability;
- f) object to processing including for direct marketing, e.g. not be subject to automated-decision making including profiling in certain circumstances.

Data Security

We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental or unlawful destruction, damage, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.

We will design and put in place procedures and technologies that maintain by default the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if it agrees to comply with those procedures and policies, or if it puts in place adequate measures itself. We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

- A) confidentiality means that only people who are authorised to use the data can access it;
- b) integrity means that personal data should be accurate and suitable for the purpose for which it is processed; and
- c) availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our central computer system instead of individual PCs.

Security procedures includes:

- i. the country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms;
- ii. the data subject has given their consent;
- iii. the transfer is necessary for one of the reasons set out in Data Protection Requirements, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject;
- iv. the transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims;
- v. the transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

Subject to the requirements above, personal data we hold may also be processed by staff operating outside the EEA who work for us, an associated company (including Global Creatures Pty Ltd) or one of our suppliers. Those staff may be engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

Disclosure and Sharing of Personal Data

We may share personal data we hold with any member of our group, i.e. our parent companies (as defined in section 1159 of the UK Companies Act 2006).

Subject Access Requests

Individuals must make a formal request for information we hold about them. Staff who receive a request should forward it to the Data Protection Compliance Manager immediately. When receiving enquiries, we will only disclose personal data we hold on our systems if we are satisfied that the identity of the enquirer is genuine through thorough checks.

Reviews and Changes to this Policy

We shall review this policy on an annual basis and reserve the right to change it at any time. Where appropriate, we will notify changes by mail, internal mail or email.