FACTORY FILMS DATA PROTECTION POLICY - GENERAL

General Data Protection Policy :

Scope of the Policy

At Factory Films we hold information protected by the General Data Protection Regulations (GDPR) and the Data Protection Bill 2018, including personal data about our employees and staff, clients, suppliers, customers and other individuals, for a variety of business purposes.

Everyone working for us has a legal obligation to ensure that we comply with the requirements of the GDPR and follow the safeguards we have implemented in order to best protect all the Personal Data we hold.

This policy sets out how the Company will seek to protect personal data and individuals' rights and obligations in relation to their personal data.

The person responsible for this policy and Data Protection compliance in the Company is Julie Heathcote.

This Policy should be regarded as a living document that may be amended by us at any time, to ensure our ongoing compliance with The General Data Protection Regulations (effective 25th May 2018) and the UK's Data Protection Act 2018.

The reasons we process personal data is to:

- Provide services to our clients (and maintain a list of them)
- Undertake research for our business
- Recruit, support, manage and pay our staff
- Manage our on-air talent and contributors
- Maintain our Accounts and Records
- Market and Promote our Goods and Services
- Respond to Enquiries and Complaints
- Maintain the security and safety of our property, premises and IT systems
- Ensure a safe working environment
- Post-production paperwork, including but not exclusive to, SilverMouse & Diamond Diversity

Definitions

Personal Data is data we gather which relates to a living individual who can be identified from that data, or from that data in conjunction with other readily available information, e.g. their name, address, images, telephone numbers, personal email addresses, date of birth, bank and payroll details, next of kin, passport particulars etc. It can also include data such as IP addresses and data automatically collected when using computers and the internet, as well as educational background (certificates, diplomas, education, skills, CV), skills, marital status, nationality, job title, contact details, references, attendance records, performance records and so on.

This data may be collected from the individual themselves or provided by other parties, and may be in paper or electronic format.

Special Category Data is data that relates to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), physical or mental health matters, sexual orientation/life, genetic and biometric data.

Criminal Records data means information about an individuals criminal convictions and offences, and information relating to criminal allegations and proceedings.

Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

Our Data Protection Principles

The GDPR protects individuals' rights concerning information about them that is held on computer. Anyone processing personal data must comply with the eight principles of good practice, which are that data must be:

- fairly and lawfully processed (in accordance with individuals' rights)
- adequate, relevant and not excessive (limited to what is necessary for the purpose of processing)
- collected only for specified, explicit and legitimate purposes (including for business purposes to comply with legal, regulatory, corporate governance obligations and good practice)
- accurate and kept up to date (we take all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay; and Individuals can ask that we correct their inaccurate personal data).
- not kept longer than necessary for its original purpose
- processed in accordance with the data subject's rights and its specified purposes
- secure (i.e. appropriate measures have been taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction or, or damage to, personal data)
- not transferred to countries or territories outside the EEA unless that area ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this, or would otherwise reasonably expect this.

Conditions for Processing Personal data

The processing of personal data will only be fair and lawful when the purpose of the processing meets a legal basis (see below) and when the processing is transparent. This means we will provide people with an explanation of how and why we process their personal data, in a Privacy notice.

Processing of personal data is only lawful if at least one of these legal conditions is met:

- Processing is necessary for the performance of a contract with the data subject or to take steps

to enter into a contract
- Processing is necessary for compliance with a legal obligation
- Processing is necessary to protect the vital interests of a data subject or another person
- 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 controller
- Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.
- If none of these legal conditions apply, the processing will only be lawful if the data subject has given their clear, explicit, consent.

Where we are required to get consent from the data subject, we will clearly set out what we are asking consent for, including why we are collecting the data and how we plan to use it. Consent will be specific to each process we are requesting consent for and we will only ask for consent when the data subject has a real choice whether or not to provide us with their data.

Consent can however be withdrawn by the individual at any time and if withdrawn, the processing must stop. Data subjects will be informed of their right to withdraw consent and it must be made as easy to withdraw consent as it is to give consent.

Privacy Notices - transparency of data protection

Being transparent and providing accessible information to individuals about how we will use their personal data is important for the Company. Privacy notices for job applicants, contributors, and visitors to our website can be found at www.factoryfilms.tv

The Privacy Notice:

- **Must be given at the point their data is collected from them** (or collected about them from other sources) and gives our identity/contact details;
- Sets out the purposes for which we hold an individual's personal data;
- Explains the legal basis for processing; if the data is to be sent outside the European Union, how long the data will be stored for;
- Highlights that sometimes the Company may be required to give information to third parties;
- Explains the individuals data subjects' rights.

This information will be provided to the individual in writing and no later than within 1 month after we receive the individuals data, unless a legal exemption under the GDPR applies.

Special Categories of Data and Criminal Records Data

In the limited cases where the Company processes special categories of data, this requires extra care and is usually only lawful when, in addition to one of the conditions above, one of the extra conditions, as listed in Article 9 of the GDPR, is met. These conditions include where:

- the processing is necessary for carrying out our obligations under employment and social security and social protection law;
- the processing is necessary for safeguarding the vital interests (in emergency, life or death situations) of an individual and the data subject is incapable of giving consent;
- the processing is carried out in the course of our legitimate activities and only relates to our members or persons we are in regular contact with in connection with our purposes;
- the processing is necessary for pursuing legal claims.
- If none of the other legal conditions apply, the processing will only be lawful if the data subject has given their explicit consent.

We will not hold information relation to criminal proceedings or offences or allegations of offences unless there is a clear lawful basis to process this data such as where it fulfills one of the substantial public interest conditions in relation to the safeguarding of children and of individuals at risk, or because it is necessary for us to carry out our statutory or regulatory obligations and exercise specific rights in relation to employment, or it meets one of the additional conditions relating to criminal convictions set out in either Part 1 or 3 of Schedule 1 of the Data Protection Regulations 2018.

Data Security

We keep personal data secure against loss, accidental destruction, misuse or disclosure and we have internal policies and controls in place to protect data.

The Company will ensure that data is not accessed except by any staff other than those who need to in the proper performance of their job.

Where other organisations process personal data as a service on our behalf, Julie Heathcote will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations.

Impact analysis exercises

Where data is processed that could result in a high risk to an individuals rights and freedoms, the Company will carry out a data protection impact assessment (DPIA) to determine the necessity and proportionality of the processing. For example, this would apply if we were to consider using CCTV cameras within the workplace, or we need to process data relating to vulnerable people, trawl data from public profiles, introduce new technology, and transfer data regularly outside the EU.

Any decision not to conduct a DPIA will be recorded. DPIAs will be conducted in accordance with the ICO's Code of Practice 'Conducting privacy impact assessments'.

Data retention periods

We retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained. The length of retention will be determined in a manner consistent with published legal and regulatory data retention guidelines.

Data retention periods are explained in our relevant Privacy Notices.

Data deletion

In our Company, Julie Heathcote is responsible for ensuring that records that are no longer required are reviewed as soon as possible so that, where appropriate, records are destroyed. Some records may instead be selected for permanent preservation, digitised to an electronic format or retained by the organisation for litigation purposes.

Transferring data internationally

There are restrictions on international transfers of personal data. Personal data must generally not be transferred outside of the European Economic Area unless the receiving country ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data, unless the data subject has given their consent and:

(a) The transfer is necessary for the performance of a contract between the data subject and the data controller, or
(b) The transfer is necessary for certain contracts with third parties, or
(c) The transfer is necessary to protect the vital interests of the data subject.

Otherwise adequate safeguards must be put in place and other conditions must be met. You should refer to Julie Heathcote if you are unsure whether this need applies.

Individuals Rights

Individuals have a number of rights in relation to their personal data:

Subject access requests

Please note that under GDPR, individuals are entitled, subject to certain exceptions, to request access to information held about them. No charges should be made to the data subject to provide this information. Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed by the Company within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system.

If you would like to make a subject access request about your own records, you should refer that request immediately to Julie Heathcote so the request can be processed.

If a subject access request is manifestly unfounded or excessive the Company is not obliged to comply with it.

Other rights

Individuals have a number of other rights in relation to their personal data. They can require the Company to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override the organisation's legitimate grounds for processing data (where the organisation relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the organisation's legitimate grounds for processing data.

To ask the Company to take any of these steps, the individual should send the request to julie.heathcote@factoryfilms.tv .

Sharing information with other organisations

We will only share personal data with other organisations or people when we have a legal basis to do so and if we have informed the data subject about the possibility of their data being shared (in a Privacy Notice), unless legal exemptions apply to informing data subjects about the sharing. Only authorised and properly instructed staff are allowed to share personal data.

On 25th May 2018 The General Data Protection Regulations become law in the UK and this policy should be seen as a living document which may be reviewed further and amended in the future to ensure it is compliant with the GDPR and the UK's Data Protection Act 2018.