# Privacy & Data Protection Policy

## Introduction

STMO, a sub-brand of Still Moving Media LLP, is committed to being fully compliant with all applicable UK and EU data protection legislation in respect of personal data, as well to safeguarding the "rights and freedoms" of persons whose information Still Moving Media LLP collects pursuant to the General Data Protection Regulation ("GDPR"). This Privacy Policy describes the way that we will use your Information.

Please read this Privacy Policy carefully to understand our policies and practices regarding your Information and how we will treat it. If you have any further questions, or if you aren't sure about anything, please feel free to get in touch with us using the contact details set out at the end of this Privacy Policy and we will be happy to help.

Personal data is anything that can directly or indirectly be used to identify an individual and includes:

- Name
- ID number
- Location data
- An online identifier
- Sensitive personal data

Sensitive personal data is referred to as "special categories of personal data" in the GDPR and includes genetic and biometric data. It no longer includes personal data relating to criminal convictions as this is now covered in its own section (Article 10). Special categories of Personal Data include:

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sex life
- sexual orientation

Additionally, Still Moving Media LLP collects CCTV recordings at its premises which is used for Crime Prevention.

## Good Practice

Still Moving Media LLP shall ensure compliance with data protection legislation and good practice, by at all times:

1. Processing personal information only when to do so is absolutely necessary for organisational purposes;

2. Ensuring that the least possible amount of personal data is collected, and that personal data is never processed unduly;

3. Informing individuals of how their personal data is or will be used and by whom;

4. Processing only pertinent and adequate personal data;

5. Processing personal data in a lawful and fair manner;

6. Keeping a record of the various categories of personal data processed;

7. Ensuring that all personal data that is kept is accurate and up-to-date;

8. Retaining personal data no longer than required by statute or regulatory body, or for organisational purposes;

9. Giving individuals the right of 'subject access', as well as all other individual rights pertaining to their personal data;

10. Ensuring that all personal data is maintained securely;

11. Transferring personal data outside of the EU only in situations where it shall be appropriately secured;

12. Applying various statutory exemptions, where appropriate;

## Use of information and data

Still Moving Media LLP use information for the purposes described in this Privacy Policy and as further disclosed to you.

In particular, we process information:

Where necessary to establish and perform our contract with you and to maintain, manage or terminate our contractual relationship, including rights management, making payments, contacting you, or your agent / representative, about your engagement where we have entered into a Studio Usage Agreement, Crew Agreement or other contractual arrangement with you.

Where necessary to comply with a legal obligation, such as:

- Carrying out necessary occupational health and safety and/or medical assessments for freelancers; and
- Administration of accounts and providing any information to tax, police and security authorities as required by law.

Information required to complete payments and financial transactions will be shared securely with third-party accountants who can share their data and privacy protection policy upon request to hello@stillmovingmedia.com

Where necessary for our legitimate interests, as listed below, and where our interests are not overridden by your data protection/privacy rights, including to specific for contributors and freelancers of any productions managed by Still Moving Media LLP:

- commission, develop, produce, publish, distribute and promote our Productions, including arranging finance, incentives or subsidies for any of our Productions;
- make a decision as to whether you are the right person for the position in the Production, or whether to accept and make use of Content that features you;
- contact you about your application, and/or casting process and/or your involvement in the Production as well as to respond to any of your communications, complaints or requests;
- investigate and resolve any concerns or other matters that may arise from your involvement with us and/or our Productions;
- protect our legitimate business interests and legal rights.
- This includes but is not limited to, use in connection with legal claims, compliance, regulatory, auditing, investigative and disciplinary purposes (including disclosure of such information in connection with any legal process or litigation or where requested by law enforcement or other relevant third parties).

Where necessary, including to specific for freelancers and companies renting studio space owned by Still Moving Media LLP:

- manage bookings for any rentals;
- make a decision as to whether you or your company are the suitable for renting any studio space;
- contact you about your rental, and/or kit requirement and/or your scheduling as well as to respond to any of your communications, complaints or requests;
- investigate and resolve any concerns or other matters that may arise from your involvement with us;
- protect our legitimate business interests and legal rights;
- This includes but is not limited to, use in connection with legal claims, compliance, regulatory, auditing, investigative and disciplinary purposes (including disclosure of such information in connection with any legal process or litigation or where requested by law enforcement or other relevant third parties).

Where necessary to prevent or detect unlawful acts, such as when carrying out background checks (e.g. checking your references and/or criminal record): such background checks will be carried out only to the extent permitted by and in accordance with applicable.

When required under applicable law, we will ask for your consent, unless there is another legal basis under applicable law for processing your information (e.g. a legitimate interest or a legal requirement), for example:

- we will usually seek your consent before sending you Marketing Communications;

Where necessary to protect the vital interests relating to you or another person (for example, avoiding serious risk of harm to you or others).

Where otherwise permitted or required under applicable law.

We will only Process the Special categories of data you share on the following grounds:
with your explicit consent, unless we are otherwise legally permitted to use your Information for another reason below;

- on the basis that you have chosen to make the personal data manifestly public, from the filming stage until after publication of the Production;
- for the purposes of freedom of expression and information, journalism and artistic expression where relevant for the Production; or
- where necessary, relevant only to contributors and talent, and permitted by law, to assess your suitability for a Production and/or analyse and monitor the diversity of our applicants. We will only process Special categories of personal data for these purposes without your consent to the extent this is permitted by applicable law.

## Individual rights

As a data subject, individuals have a number of rights in relation to their personal data.

### *Subject access requests*

Individuals have the right to make a subject access request. If an individual makes a subject access request, Still Moving Media LLP will tell him/her:

- whether or not his/her data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- to whom his/her data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long his/her personal data is stored (or how that period is decided);
- his/her rights to rectification or erasure of data, or to restrict or object to processing;
- his/her right to complain to the Information Commissioner if he/she thinks the organisation has failed to comply with his/her data protection rights; and
- whether or not the organisation carries out automated decision-making and the logic involved in any such decision-making.

Still Moving Media LLP will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless he/she agrees otherwise.

To make a subject access request, the individual should send the request
to hello@stillmovingmedia.com
In some cases, Still Moving Media LLP may need to ask for proof of identification before the request can be processed. The organisation will inform the individual if it needs to verify his/her identity and the documents it requires.

Still Moving Media LLP will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the organisation processes large amounts of the

individual's data, it may respond within three months of the date the request is received. The organisation will write to the individual within one month of receiving the original request to tell him/her if this is the case.

If a subject access request is manifestly unfounded or excessive, Still Moving Media LLP is not obliged to comply with it. Alternatively, the organisation can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the organisation has already responded. If an individual submits a request that is unfounded or excessive, the organisation will notify him/her that this is the case and whether or not it will respond to it.

## Collection of CCTV recordings

### Overview

Still Moving Media LLP collects CCTV recordings at its premises, Unit 6, Furlong Park, GL52 8TW for the purposes of crime prevention.

The CCTV system is owned by Still Moving Media, Unit 6, Furlong Park, GL52 8TW and managed by the organisation and its appointed third-party contractor, A&E Fire & Security.

Under current data protection legislation Still Moving Media LLP is the 'data controller' for the images produced by the CCTV system.

Still Moving Media is registered with the Information Commissioner's Office and the registration number is Z5654762. The CCTV system operates to meet the requirements of the Data Protection Act and the Information Commissioner's guidance.

The organisation director's are responsible for the overall management and operation of the CCTV system, including activities relating to installations, recording, reviewing, monitoring and ensuring compliance with this policy. The CCTV system operates both outside and inside the premises.

Details of the number of cameras can be requested at hello@stillmovingmedia.com

Signs are placed at all pedestrian and vehicular entrances in order to inform employees, contractors, freelancers, clients, visitors and members of the public that CCTV is in operation. The signage indicates that the system is managed by Still Moving Media LLP and that the recordings are made 24-hours a day.

The organisation director's are responsible for ensuring that adequate signage is erected in compliance with the ICO CCTV Code of Practice. Cameras are not sited to focus on private residential areas. Where cameras overlook residential areas, privacy screens will be fitted.

The CCTV system is operational and is capable of being monitored for 24 hours a day, every day of the year. Any proposed new CCTV installation is subject to a Data Protection Impact Assessment. Any new CCTV Camera installation is subject to a privacy assessment.

Overview

The principal purposes of the organisation's CCTV system are as follows:

for the prevention, reduction, detection and investigation of crime and other incidents; - to ensure the safety of staff, clients, freelancers and visitors;
to assist in the investigation of suspected breaches of regulations by staff or visitors; and
the monitoring and enforcement of traffic related matters.

Still Moving Media LLP seeks to operate its CCTV system in a manner that is consistent with respect for the individual's privacy.

Images are recorded centrally on servers located securely in the Still Moving Media LLP Data Centre and are viewable only by permitted employees in areas with limited access and access control. Additional staff may be authorised by the organisation director's to monitor cameras sited within their own areas of responsibility on a view only basis. The cameras installed provide images that are of suitable quality for the specified purposes for which they are installed and all cameras are checked weekly to ensure that the images remain fit for purpose and that the date and time stamp recorded on the images is accurate.

All images recorded by the CCTV System remain the property and copyright of Still Moving Media LLP

Access to and disclosure of images to third parties. A request for images made by a third party should be made in writing to hello@stillmovingmedia.com

### Retention of images

Unless required for evidential purposes, the investigation of an offence or as required by law, CCTV images will be retained for no longer than 30 days from the date of recording. Images will be automatically overwritten after this point.

### Complaints

Complaints concerning the use of its CCTV system or the disclosure of CCTV images should be made in writing to the management team of Still Moving Media LLP at: hello@stillmovingmedia.com

All appeals against the decision of the management team should be made in writing to the organisation director's at studio@stillmovingmedia.com

## Storage of media files

### Overview

This policy supports the objectives of the overarching Privacy & Data Protection Policy.

Still Moving Media LLP store all media files from all Productions in a secure storage server as well as a secure storage safe. Some files may be stored off-site with employees of the organisation during the post-production phase of the Production.

### Responsibility

The responsibility for the storage of media files from Productions is with the Post-Production team at Still Moving Media LLP.

Appropriate handling of media files is the responsibility of all employees, consultants, temporary staff and sub-contractors of Still Moving Media LLP.

## Scope

This policy is concerned with all media files, digital and non-digital, and covers all media content within Still Moving Media LLP that is or may be:

1. stored on computers and servers;
2. transmitted across networks;
3. printed out or written on paper;
4. sent internally or externally by post, courier, or fax;
5. stored on removable and other electronic media;

## Information Access

Internal and external access to media files held by the organisation, and to the systems within which it is held, is managed by the Post-Production team and is monitored at all times.

i. Operational information is either generally available to the public or all staff on a need-to-know basis, as decided by their line manager.
ii. Sensitive data is available only to employees and freelancers who have a business need to know the information, and with the written approval of the management team.

Still Moving Media LLP have put into place the following protocols for safe and secure management of media files:

Where access to sensitive data has been authorised, use of such data shall be limited to the purpose required to perform the organisation's business.

Where an employee or freelancer who has access to sensitive data either leaves or has their authorisation removed e.g. as a result of a change of role, their status must be updated within 24 hours. e.g., by changing access control lists and account access.

Information should be stored throughout its existence in an environment suited to its format and privacy classification, to ensure its preservation from physical harm or degradation and its security from loss or unauthorised access.

Information, whether original or duplicate, should never be kept outside Still Moving Media LLP's processes (e.g. on personal computers, on CDs or USB keys) except in extreme circumstances such as a temporary off-line copy driven by a business need to work off-site or off-line, or for authorised transfer to other users or systems.

Information in all formats should be stored in conditions that protect it from threats to its physical integrity through unnecessary wear and tear; specific threats such as fire, flooding, and magnetic fields; and environmental extremes or fluctuations. Where appropriate, special storage equipment and environments should be used.

Information should be stored in systems and according to classifications, frameworks and procedures that enable it to be readily identified and retrieved throughout its existence.

Information held in digital formats should be managed and stored in such a way as to ensure usability and accessibility through time. This may involve migration of information between environments and systems, conversion to current software versions, or conversion from obsolete to current formats.

Physical access to information should be restricted by locking it in rooms, cabinets, drawers, and other storage areas or units, and by ensuring that files and computer monitors are not left open to general or casual view.

Protection from unauthorised access may require mechanisms such as password protection or encryption of digital files and data, and sign-in sheets or request dockets for access to non-digital information.

Where information is stored on a mobile device (e.g. HDD drive, SSD drive, laptop), special care must be taken to ensure that the device is physically protected from theft, loss, or damage, particularly if it is transferred or used away from Still Moving Media LLP studios.

Still Moving Media LLP employees must not use cloud services to store files containing personal, sensitive or confidential information because of the risks stated in this policy, unless on the following approved list of services:

- WeTransfer
- Microsoft Office 365 Suite
    1. SharePoint
    2. Outlook
    3. OneDrive
- Vimeo
- Dropbox
- Asana
- Miro

## Data security

The organisation takes the security of personal data seriously. The organisation has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

## Data breaches

If the organisation discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. The organisation will record all data breaches regardless of their effect.

## Individual responsibilities

Individuals are responsible for helping the organisation keep their personal data up to date.

Individuals should let the organisation know if data provided to the organisation changes, for example if an individual moves house or changes his/her bank details.

Individuals may have access to the personal data of other individuals (and of our customers and clients) in the course of their (employment, contract, volunteer period, internship or apprenticeship). Where this is the case, the organisation relies on individuals to help meet its data protection obligations to staff (and to customers and clients).

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from the organisation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;
- not to store personal data on local drives or on personal devices that are used for work purposes; and
- to report data breaches of which they become aware to hello@stillmovingmedia.com immediately.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the organisation's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or client data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.