Fictional Company Productions Ltd
Registered company number 13533127
Summit House, 170 Finchley Road, London NW3 6BP
info@fictionalcompany.co.uk

Data Protection Policy

February 2022

Introduction

Fictional Company takes its responsibilities with regard to the management of the requirements of the General Data Protection Regulation (GDPR) very seriously, and is registered with the Information Commissioner's Office. This policy sets out how the Company manages those responsibilities, and prepares the Company to enter into data-sharing agreements with partner organisations.

Fictional Company obtains, uses, stores and otherwise processes (or expects to) personal data relating to (potential, current and former) staff, contractors, supporters, donors, website and mailing list users, and audiences (including audience data legally shared via third parties and co-producers), collectively referred to in this policy as data subjects. When processing personal data, the Company is obliged to fulfil individuals' reasonable expectations of privacy by complying with GDPR and other relevant data protection legislation (data protection law).

This policy therefore seeks to ensure that Fictional Company:

1. Is clear about how personal data must be processed;
2. Complies with the data protection law and with good practice;
3. Protect the Company's reputation by ensuring the personal data is processed in accordance with data subjects' rights;
4. Protects the Company from risks of personal data breaches and other breaches of data protection law.

Scope

This policy applies to all personal data Fictional Company processes, regardless of the location where that personal data is stored (e.g. on an employee's own device) and regardless of the data subject. All staff and others processing personal data on the Company's behalf must read this policy. Failure to comply with this policy may result in disciplinary action.

The Company currently has a sole director, who will serve is Data Protection Officer (DPO) for the purposes of this policy.

Personal data protection principles

FICTIONAL COMPANY

When you process personal data, you should be guided by the following principles, which are set out in the GDPR. The Company is responsible for, and must be able to demonstrate compliance with, the data protection principles listed below. Those principles require personal data to be:

- processed lawfully, fairly and in a transparent manner (Lawfulness, fairness and transparency).
- collected only for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes (Purpose limitation).
- adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data minimisation).
- accurate and where necessary kept up to date (Accuracy).
- not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data is processed (Storage limitation).
- 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).

Data Subjects' Rights

Data subjects have rights in relation to the way we handle their personal data. These include the following rights:

- where the legal basis of our processing is Consent, to withdraw that Consent at any time (such as to have details erased from a mailing list);
- to ask for access to the personal data that we hold (such as a personnel file)
- to prevent our use of the personal data for direct marketing purposes (such as website users who have not provided consent to receive marketing materials)
- to object to our processing of personal data in limited circumstances
- to ask us to erase personal data without delay, if it is no longer necessary in relation to the purposes for which it was collected or otherwise processed; if the only legal basis of processing is Consent and that Consent has been withdrawn and there is no other legal basis on which we can process that personal data; if the data subject objects to our processing where the legal basis is the pursuit of a legitimate interest or the public interest and we can show no overriding legitimate grounds or interest; if the data subject has objected to our processing for direct marketing purposes; or if the processing is unlawful.
- to ask us to rectify inaccurate data or to complete incomplete data;
- to restrict processing in specific circumstances e.g. where there is a complaint about accuracy;
- to ask us for a copy of the safeguards under which personal data is transferred outside of the EU;
- the right not to be subject to decisions based solely on automated processing, including profiling, except where necessary for entering into, or performing, a contract; it is based on

the data subject's explicit consent and is subject to safeguards; or is authorised by law and is also subject to safeguards;
- to prevent processing that is likely to cause damage or distress to the data subject or anyone else;
- to be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;
- to make a complaint to the ICO; and
- in limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format.

You must verify the identity of an individual requesting data under any of the rights listed. Requests (including for data subject access – see below) must be complied with, usually within one month of receipt. A charge can be made for dealing with requests relating to these rights only if the request is excessive or burdensome.

Responsibilities & procedures

All staff processing data for or on behalf of Fictional Company must comply with the requirements of this policy, including that:

- all personal data is kept securely (typically either on the Company's password-protected cloud data storage, or within a secure third-party platform in the case of mailing list or website user data, which must be compliant with current GDPR law);
- no personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party;
- any (potential) data protection breaches, or any queries regarding data protection, including subject access requests and complaints, are handled and reported promptly;
- in general, common sense and good care will be sufficient principles to follow given the Company's relatively limited role in data processing, but that where there is uncertainty around a data protection matter, appropriate legal advice is sought.

In practice, the Company's legal requirements and expectations under the terms of this policy can be met in the course of general business by ensuring:

- that website and mailing list data is managed by GDPR-compliant password-protected platforms providing clear information on the expected use (eg marketing, fundraising) and scope for data subject consent (and withdrawal, eg through an 'unsubscribe' option);
- that all other data is stored on password-protected platforms;
- that staff and contractor data is only kept insofar as it is necessary for meeting legal and operational responsibilities (such as contracting and payment);
- that personal data relating to donors and supporters is only kept insofar as it is necessary to meet legal, financial reporting and taxation requirements;
- that no personal data is shared with any third party without explicit consent, and any reasonable and legitimate requests for data erasure or limitation are handled swiftly.

FICTIONAL COMPANY

This policy statement and/or the procedures for its implementation may be altered at any time by the Company director(s). The statement and the procedures are to be reviewed annually, or in line with significant changes to the Company's activities and/or employees.