Papatango Theatre Company Ltd
Data Protection Policy in Accordance with the EU General Data Protection Regulation (GDPR)

Context and Overview

Key Details

- Policy prepared by: Chris Foxon
- Approved by board / management on: 30/04/2018
- Policy became operational on: 01/05/2018
- Next review date: 30/04/2019

Introduction

Papatango Theatre Company Ltd needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees, audiences, participants, and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards. It ensures and provides proof of the company's compliance with the European General Data Protection Regulation (GDPR).

This policy also protects the rights of staff, customers and partners, and allows the company to be open about how it stores and processes individuals' data. This policy protects the company from the risks of a data breach.

Personal data is defined as data that can identify a living individual and/or that is directly linked to them. Anything that is anonymised is not personal data; as soon as data is disconnected from a named or specific individual, and they can no longer be identified by it, it is no longer regarded as personal data. This anonymised data is not the subject of this policy.

The key principles of the GDPR, which this policy reflects, are:

- Fair, lawful and transparent
- Purpose limitation
- Data minimisation
- Accuracy

- Data retention
- Data security
- Accountability

People, Risks and Responsibilities

Policy Scope

This policy applies to:

- The head office and any other working environments of Papatango Theatre Company Ltd
- The board of trustees, staff and volunteers of Papatango Theatre Company Ltd
- All contractors, suppliers and other people working on behalf of Papatango Company Ltd

Data Protection Risks

This policy helps to protect Papatango Theatre Company Ltd from:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.
- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.
-

Responsibilities

Everyone who works for or with Papatango Theatre Company Ltd has some responsibility for ensuring data is collected, stored and handled appropriately. Everyone who handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

- The **board of trustees** is ultimately responsible for ensuring that Papatango Theatre Company Ltd meets its legal obligations.
- The **producer** is responsible for:
    - Keeping the board updated about data protection responsibilities, risks and issues.

- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Handling data protection questions from staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the data Papatango Theatre Company Ltd holds about them (also called 'subject access requests').
- Checking and approving any contracts of agreements with third parties that may handle the company's sensitive data.
- Ensuring all systems, services and equipment used for storing data meets acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.
- Maintaining records of processing activities.
- Updating other organisations. If Papatango Theatre Company Ltd possesses inaccurate personal data and has shared this with another organisation, said organisation must be informed to update their personal records.
- Contacting the ICO to seek its opinion if a DPIA indicates that the data processing is high risk, and the company cannot sufficiently address these risks.
- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets like newspapers.
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

General Staff Guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines.

- In particular, strong passwords must be used and they should never be shared.
- There should be no sharing of accounts.
- Anyone who uses their personal laptops/emails/mobiles must ensure that no personal data is stored directly on these devices.
- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted, otherwise disposed of, or archived as discussed below.
- Employees should request help from their line manager or the producer if they are unsure about any aspect of data protection.
- All breaches must be reported to the ICO and the individuals to whom the data belongs.
- A commitment to continuous improvement of a data protection management system is in place.
- Obligatory attendance at necessary training events in relation to this policy will be mandated.
-

Data Collection

Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes.

On the basis of its most recent data audit in February 2018, Papatango Theatre Company Ltd's data consists of:

- Papatango New Writing Prize entrants' contact details.
- Workshop participants' contact details.
- Open audition participants' contact details.
- The contact details of those on the company's mailing list.
- Anyone with whom the company has email or phone contact.
- Third party audience data provided to the company from venues, co-producers or partners.
- The contact details of job applicants.

All trustees, staff or volunteers of the company should follow these guidelines to ensure effective regulation of this data or legal and ethical collection of new data:

- Prize entrants and/or workshop or open audition participants will only be asked to share their data with Papatango Theatre Company Ltd when they apply to be part of a particular project. They will thereafter only be contacted about, or their data otherwise processed to deliver, this particular project, as it is a legitimate interest for the company to liaise with them about their specific application. As soon as Papatango Theatre Company Ltd has adequately managed and completed a project, all relevant personal data will be disposed of (see below).
- Notes taken on a job applicant during an interview constitute personal data. If the company wishes to keep this information on file for future relevant openings, the candidate must be asked which specific data can be kept and give their consent to this.
- The mailing list will only include people who have actively given consent by opting to join the list. This consent will be documented via the service provided by Mailchimp, which will track the location and time of each individual opt-in. The mailing list will be used only to disseminate information that is directly relevant to the work of Papatango Theatre Company Ltd. The ability to opt-out or resign from the mailing list will be clearly signposted on every communication from the company.
- The company will never use auto opt-in or pre-ticked boxes.
- Any request for consent will be separate and distinct from other terms and conditions.
- Individuals must be over the age of 16 to opt-in to any services run by the company.
- The company will always make the intent of the data use clear to those who do opt-in or give consent i.e. that it will be used to receive regular mailouts and communications from the company, or to manage a relevant project.
- Individuals will be able to withdraw their consent to the company's processing or use of their data at any time and without detriment.
- No data will be shared with any other party, organisation or individual unless those concerned have given express permission.
- At all times that data is collected, this will be accompanied by a clear statement about the information the company will collect and how it will be collected. Moreover, a privacy notice will include: identify and contact details of the data processor; purpose and legal basis for processing the data; how the data will be processed; who will be involved in processing the data; how long it will be kept; and the right of the individual to object to processing.

Providing Information

Papatango Theatre Company Ltd aims to ensure that before collecting data individuals are aware that their data is being processed and that they understand:

- How the data is being used.
- Where it is being stored.
- How to exercise their rights.
- The company's lawful basis for processing the data.
- The company's data retention periods.

Individuals must also be aware of their following rights:

- The right to be informed
    - Subjects must be informed about the collection and processing of their personal data in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
- The right of access
    - Data subjects have the right to access their personal data, to see what is being held and what is being done with it. A SAR must be submitted to access this data.
- The right to rectification
    - Data subjects have the right to correct inaccurate personal data. Inaccurate or incomplete data must be erased or amended within one month of the notice, or two if the request is complex. If data has been shared with third parties, they must be informed so it can be corrected.
    - However, the right to be informed about third parties the company has contacted is a right that may or may not be requested by the data subject. It's not an obligation for the company to provide this information in all cases.
- The right to erasure, also known as the right to be forgotten. An individual can request the deletion or removal of personal data if the following conditions are met:
        - There is no compelling reason for its continued processing.
        - The data subject withdraws consent.
        - Their data was unlawfully processed.
- The right to restrict processing

    - Under certain circumstances, such as when there's a dispute about the accuracy of the data, people have the right to restrict processing. When it is restricted, the company is permitted to store the personal data, but not to process it in any other way. The company must hold just enough personal data to ensure that the restriction is maintained, and all third parties with whom data has been shared must be informed.

- The right to data portability
    - This allows individuals to get hold of and reuse their personal data for their own purposes across different services. A copy of their data must be given in a format that they can use or the company must transmit it directly to another data controller.

- The right to object
    - Individuals must be informed about their right to object when data is collected. If an objection is received, the company must immediately stop processing data.
    - There are no grounds to refuse to stop processing personal data for direct marketing.

- The right not to be subject to automated decision-making, including profiling
    - Individuals are given certain protections against the risk that a potentially damaging decision is made by a computer without the involvement of a human.
    - This extends to profiling and processing that analyses or predicts aspects such as health, behaviour or performance at work.

- The right to complain to the ICO if they think there is a problem with the way the company is handling their data.

This information must be provided in concise, easy to understand and clear language.

Data Storage

These rules describe how and where data should be safely stored. Data may only be stored if it is essential, not in the event that it may hypothetically become useful in the future.

Paper Data

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet. Keys to these filing systems should be kept secure.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like a printer or on a desk.
- Data printouts should be shredded and disposed of securely using confidential waste facilities when no longer required.

Electronic Data

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees, not even with IT staff.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used. Keys to these filing systems should be kept secure.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing service.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.
- Ask IT to wipe files from external drives.

Data Use

Personal data is of no value to Papatango Theatre Company Ltd unless the company can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft. To guard against this, these guidelines should be followed:

- When working with personal data, employees or volunteers should ensure the screens of their computers are always locked when left unattended.

- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure. Instead, links to secure areas on the corporate system or corporate server should be used.
- When emails are sent, the email trail must be reviewed before replying.
- Personal data should never be transferred outside of the European Economic Area.
- Personal data should never be forwarded to anyone who does not have a valid reason for seeing it.
- The company must consider whether an individual would consider the purpose for which you intend to use their data as being fair.
- Employees or volunteers should not save copies of personal data to their own computers. Always access and update the central copy of any data.
- Employees or volunteers must be aware of the surroundings when working with personal data, particularly in public areas.
- Seek advice on sending hard copies of personal data securely.

Personal data must be handled only in ways that the individual would expect. One or more of these conditions must be met in order for data to be processed:

- The individual has consented.
- The processing is necessary so an individual can enter into a contract or in relation to an existing contract.
- The processing is necessary because of a legal obligation.
- The processing is necessary to protect the individual's 'vital interests' e.g. in cases of life or death.
- The processing is necessary to delivery justice or to exercise statutory, governmental, or other public functions.
- The processing is in accordance with the 'legitimate interests' condition.

Personal data must be processed in a way that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Data Accuracy

The law requires Papatango Theatre Company Ltd to take reasonable steps to ensure data is kept accurate and up to date. When data is no longer necessary, it should be erased or rectified without delay.

The more important it is that the personal data is accurate, the greater the effort Papatango Theatre Company Ltd should put into ensuring its accuracy. It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets as these may result in confusing or contradictory records.
- Staff should take every opportunity to ensure data is updated.
- Papatango Theatre Company Ltd will make it easy for data subjects to update the information held about them.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
- The company will document all the purposes for which personal data is held and what the lawful basis is that applies.

Subject Access Requests (SAR)

All individuals who are the subject of personal data held by Papatango Theatre Company Ltd are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

If an individual contacts the company requesting this information, this is called a subject access request. Individuals will not be charged for a subject access request. The data controller will aim to provide the relevant data within a month (two, for a complex request), in a structure commonly used and machine-readable format.

The company must supply:

- Confirmation that the individual's personal data are being processed.
- The purposes of the processing.
- The categories of data being processed.
- Who their data might be shared with.
- How long their data will be stored.

- The source of their data.
- A copy of their data.
- Their rights (to erasure, rectification).
- How automated decisions are made.

The company can refuse or charge for requests that are manifestly unfounded or excessive. If a request is refused, the individual must be told why and that they have the right to complain to the supervisory authority and to a judicial remedy. This must be done without undue delay and at the latest, within one month.

The company must always verify the identity of anyone making a subject access request before handing over any information.

Disclosing Data

In certain circumstances, personal data may be disclosed to law enforcement agencies without the consent of the data subject. For example, HMRC can ask an employer to hand over employee data without needing the employee's consent if they are investigating a tax matter.

Under these circumstances, Papatango Theatre Company Ltd will disclose requested data. However, the company must be convinced that the request is legitimate, seeking assistance from legal advisers where necessary.