Data Management Policy

This document shows the approach we take at Regional Screen Scotland towards data protection. It shows how we work towards, and maintain compliance with, data protection regulations.

Context and overview

Key details:

- Policy prepared and monitored by: RSS Staff
- Approved by Board/management: Board Meeting 4 April 2018
- Policy operational from: 25 May 2018
- Next review date: May 2019
- Ongoing monitoring of Data Protection practices

Introduction:

Regional Screen Scotland needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how these personal data must be collected, handled and stored to meet with RSS’s data protection standards – and to comply with the law.

Why this policy exists:

This data management policy ensures Regional Screen Scotland

- Complies with data protection law and follows good practice
- Protects the rights of customers, staff and partners
- Is transparent about how it stores and processes individuals’ data
- Protects itself from the risks of a data breach
Data protection law:

The General Data Protection Regulation (GDPR) applies in the UK and across the EU from May 2018. It requires personal data shall be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals;
2. Collected for specified, explicit and legitimate purposes and processed in a manner that is compatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research or statistical purposes shall be considered to be compatible with the initial purposes;
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by GDPR in order to safeguard the rights and freedoms of individuals;
6. Processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
7. The controller (ie RSS) shall be responsible for, and be able to demonstrate, compliance with the principles.

People and responsibilities

Everyone at Regional Screen Scotland contributes to compliance with GDPR. It is important to RSS that staff prioritise and support company efforts to comply with GDPR. RSS needs to ensure that staff understand what is expected of RSS under GDPR. To that end we will be:

- Keeping senior management and Board updated about data protection issues, risks and responsibilities
- Documenting, maintaining and developing the organisation’s data protection policy and related procedures, on an ongoing basis
- Embedding ongoing privacy measures into corporate policies and day-to-day activities, throughout the organisation and within each area of work that processes personal data. The policies themselves will stand as proof of compliance
- Disseminating the policy across the organisation, and giving information to staff at staff meetings
- Dealing with subject access requests, deletion requests and queries from clients, stakeholders and data subjects about data protection related matters
• Checking and approving contracts or agreements with third parties that may handle the company’s sensitive data
• Ensuring all systems, services and equipment used for storing data meet 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, to ensure their compliance with obligations under the regulations
• Developing privacy notices to reflect the lawful basis for fair processing, ensuring that intended uses are clearly articulated, and that data subjects understand how they can give or withdraw consent, or else otherwise exercise their rights in relation to the company’s use of their data
• Ensuring that audience development, marketing, fundraising and all other initiatives involving processing personal information and/or contacting individuals abide by the GDPR principles

**RSS has designated one post, that of Administrator, to have prime responsibility for ensuring compliance with the terms of GDPR**

The tasks of this post are:

• To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws
• To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits
• To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc)

**Scope of personal information to be processed**

In the course of its work RSS processes personal information about staff and Board members, customers, suppliers, sponsors, funders and partners:

• We process all of the following:
  o names of individuals
  o postal addresses
  o email addresses
  o telephone numbers
  o payment information
  o other information relating to individuals eg emergency contacts for staff
  o personal information from customers in surveys, as required by funders and other bodies for monitoring purposes

**Data Audit Spreadsheet** - RSS keeps a Data Audit spreadsheet which documents how the data we hold are collected, processed and stored. It is updated as new projects arise or
there are changes to projects, and also as our technical infrastructure is developed and altered. It is reviewed annually.

The Audit, and regular reviews of it, will ensure that the data are checked for accuracy, that it is relevant, that it is not excessive, that it is up-to-date and not kept for longer than is necessary

We do not consider that any of our current practices are covered by “Industry Suppression services” We will review this on a regular basis.

Uses and conditions for processing

Below is a summary of the over arching categories of data we collect and process.

<table>
<thead>
<tr>
<th>Outcome/Use</th>
<th>Processing required</th>
<th>Data to be processed</th>
<th>Conditions for processing</th>
<th>Evidence for lawful basis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ticket buying</td>
<td>Through the SM website customers have their data processed by Veezi, Payment Express and World Pay.</td>
<td>Choice of tickets, names, emails, phone numbers (optional) and card details.</td>
<td>Contract</td>
<td>A customer voluntarily enters their data to purchase tickets. Dated records of the transactions are in Veezi, Payment Express &amp; World Pay.</td>
</tr>
<tr>
<td>SM e-Newsletters</td>
<td>Using MailChimp the Screen Machine e-newsletter is sent to lists of customers who have signed up for it via the website.</td>
<td>Names and email addresses.</td>
<td>Consent</td>
<td>People sign themselves up to receive the e-newsletters and MailChimp has a record of the date they do this. They can unsubscribe with every correspondence.</td>
</tr>
<tr>
<td><strong>Surveys &amp; Audience Research</strong></td>
<td>In the SM e-newsletter to those signed up for it, we add a link, if they should wish to follow it, to surveys. This link will take a customer to a survey in SurveyMonkey. Our Surveys are currently run by Social Value Lab to ensure anonymity.</td>
<td>Names and email addresses are in the care of RSS, in Mailchimp. Data in the surveys goes direct to Social Value Lab. RSS only sees anonymised versions of them.</td>
<td>Consent</td>
<td>People sign up to receive our e-newsletter and follow the link to a survey if they wish to do so. They can unsubscribe with every correspondence. MailChimp and SurveyMonkey have records of the dates of signing.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>Poster distribution</strong></td>
<td>Using a mailing list for each location, Screen Machine’s posters are sent out in the post.</td>
<td>Names and addresses, mostly businesses, some private.</td>
<td>Legitimate Business/</td>
<td>The mailing list is contacted annually to check if they would like to opt out/ make changes. There are email records of this. Under GDPR 2018 mail can be sent without consent but we consider it good practice to get consent.</td>
</tr>
<tr>
<td><strong>Recruitment &amp; Personnel functions</strong></td>
<td>Data are processed for the selection of interviewees from applications. Data are processed to offer and confirm employment and to enable PAYE and expenses payments to be made.</td>
<td>Data can include names, addresses, email and phone numbers. D.O.B, payment info, health info and CVs. Equal opporunties statement for monitoring purposes</td>
<td>Consent</td>
<td>Data are acquired at the recruitment stage by ‘consent’ as people willingly apply direct to us for positions. Employees’ data are held through having a ‘contract’ with them that is dated. Equal ops data are anonymised.</td>
</tr>
<tr>
<td><strong>Finance dept functions</strong></td>
<td>Making payments, processing income.</td>
<td>Names, addresses, emails, phone numbers and bank details.</td>
<td>Contract</td>
<td>Emails and paperwork are dated and filed. Bank transactions dated.</td>
</tr>
<tr>
<td>Community Cinema Development</td>
<td>To communicate as part of our core business by emails, newletters and surveys to Scotland's cinema &amp; film festival communities. Making use of Mailchimp and SurveyMonkey. Also putting them “on the map” on the RSS website.</td>
<td>An excel spreadsheet of data with organisations’ names and organisers’ names. Also emails and phone numbers – some business, some personal.</td>
<td>Legit Business</td>
<td>We have a database of contacts which aims to cover all the cinema and film festival activity taking place in Scotland. With every communication to them they are given the opportunity to update their info or be deleted</td>
</tr>
<tr>
<td>Devolved funding</td>
<td>Calls for applications to devolved funding schemes we administer via email and social media.</td>
<td>Names, email, addresses, and phone numbers - some business, some personal.</td>
<td>Legit Business in the first place.</td>
<td>It is our publicly funded remit to reach all cinemas/ festivals with info about funding to aid their development. Dated emails and paper records are kept of correspondence with the option to not be contacted again.</td>
</tr>
<tr>
<td>Sponsors and funders</td>
<td>Emails, press releases, contracts and phone calls to existing sponsors and funders.</td>
<td>Organisations and their personnel names, emails, addresses, phone numbers.</td>
<td>Contract with the successful groups.</td>
<td>Existing sponsors and funders have signed contracts with us and there’s dated emails and paper proof of this.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Contract</td>
<td>We are required to raise income to meet our organisational aims. Dated emails and paper records are kept of correspondence with the option to not be contacted again.</td>
</tr>
</tbody>
</table>
Privacy Impact Assessments

RSS will undertake Privacy Impact Assessments at the outset of new projects. These Assessments will help us identify the most effective ways to comply with our data protection obligations and meet individuals’ expectations of privacy, and protect against the risk of harm through use or misuse of personal information. Our Assessments will help us to identify and fix problems at an early stage, reducing the associated costs and damage to our reputation which might otherwise occur.

Data Sharing

Our policy is not to share any personal data with third parties. At present none of our activities involve data sharing with third parties, and if in the future we change this policy we will ensure that any such practices are fully compliant with the terms of GDPR.

Security measures

The RSS offices are opened with a pass key that all staff have. There is a lockable cabinet in the office for paperwork which includes personal data.

IT security is maintained by our IT consultant. The server and office computers are fully encrypted and password protected. All documents are backed up to a cloud storage server. The cloud based backups are fully encrypted. RSS’s IT consultant keeps all of our administration passwords and encryption keys in a secure encrypted password manager that can only be accessed by them using their fingerprint, Face ID or a password with more than 10 characters. They access this information on either their laptop or phone which are both fully encrypted (including backups).

Subject access requests aka SARs

All individuals who are the subject of data held by RSS 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

Requests can be made by direct contact with the office info@regionalscreenscotland.org

All SARs will be free of charge, except in those circumstances allowed by the GDPR. All requests will be responded to within one month.
The right to be forgotten

Except where a financial audit trail is required by law and certain other restrictions in GDPR, it is mostly the case that individuals have a right for their personal details to be deleted from our records at their request. Where ticket buying customers to Screen Machine are concerned, if they wish to have their information removed from the box office system, we will contact Veezi on their behalf and Veezi will carry out the request. For any customers to RSS requesting to have their data erased from our files – we will do this within one month as required by the GDPR guidelines.

Requests can be made by direct contact with the office info@regionalscreenscotland.org

Privacy notices

RSS aims to ensure that individuals are aware that their data are being processed, and that they understand:

- Who is processing their data
- What data are involved
- The purpose for processing that data
- The outcomes of data processing
- How to exercise their rights.

To these ends RSS has privacy statements, setting out how data is collected and processed by the company.

The privacy statements will be linked up to where ever data are being collected by RSS

Ongoing documentation of measures to ensure compliance

This Policy will be reviewed whenever any changes occur to RSS personnel, practices, policies, or technical infrastructure that have an impact on any of the information given.

The policy will be reviewed annually but will also be subject to ongoing monitoring.

GDPR issues will be incorporated into the quarterly Risk Assessments reports to the Board.

ENDS

Adopted 4th April 2018