

The Regal Cinema Melton Data Management Policy

1. Context and overview

Key details:

- Policy prepared by: Amanda Munding, Director of Regal Cinema Melton Limited and appointed Data Protection Officer (DPO)
- Policy became operational on: 25th May 2018
- Next review date: 25th May 2019

Introduction:

The Regal Cinema 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 this personal data must be collected, handled and stored to meet the company's data protection standards - and to comply with the law.

Why this policy exists:

This data management policy ensures The Regal Cinema:

- 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 not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research or statistical purposes shall not be considered to be incompatible 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 shall be responsible for, and be able to demonstrate, compliance with the principles.

2. Who? People and responsibilities

Everyone at The Regal Cinema contributes to compliance with GDPR. There is a clear understanding of the requirements and accountability of the organisation sufficient to prioritise and support the implementation of compliance. These responsibilities include (but are not necessarily limited to):

- 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, in line with agreed schedule
- Embedding ongoing privacy measures into corporate policies and day-to-day activities, throughout the organisation and within each business unit that processes personal data. The policies themselves will stand as proof of compliance.
- Dissemination of policy across the organisation, and arranging training and advice for staff
- Ensuring subject access requests, deletion requests and queries from clients, and data subjects about data protection related matters have been adhered to by staff
- Checking and approving contracts or agreements with third parties that may handle the company's sensitive data
- 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 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

Data Protection Officer (DPO) - the person responsible for fulfilling the tasks of the DPO in respect of The Regal Cinema is Amanda Munding, Director. The DPO will:

- Inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws
- 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
- Be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc)

3. Scope of personal information to be processed

While a Member of The Regal Cinema the following information will be stored:

- names of individuals
 - postal addresses of individuals
 - email addresses
 - telephone numbers
 - identifiers (Single, Joint, Family Member)
 - any relevant notes taken with regards to membership or booking
- The information is stored on an excel database on the box office and back office computers.
 - To ensure accuracy of information, relevant for purpose, not excessive and up-to-date records will be revised and updated on a monthly basis.
 - To protect sensitive special categories of personal information that it is necessary for The Regal Cinema to process the database is only accessible via a password.

4. Uses and conditions for processing

Types of processing carried out by The Regal Cinema, intended purpose for that processing, the data to be processed and what is the lawful basis for processing:

| Outcome/Use | Processing required | Data to be processed | Conditions for processing | Evidence for lawful basis |
|---------------------------------|--|---------------------------------|---|--|
| <i>Monthly brochure mailing</i> | <i>Mail-merge of name address details from patron database</i> | <i>Name and address details</i> | <i>Consent given by purchasing membership</i> | <i>Evidence of date consent given recorded on database & stored for one year</i> |
| | | | | |

Consent

- By purchasing membership and providing personal information, consent is given for The Regal Cinema to use this information to contact customers with regards to bookings and membership
- The date of joining the Membership scheme will be recorded on the database
- All personal information and consent to store information will cease at the time of membership expiry. Personal data will be removed one year after expiry unless otherwise requested to remove prior to this under the 'Right to be forgotten' (GDPR May 2018)

5. Privacy Impact Assessments

- The Data Protection Impact Assessment (DPIA) for The Regal Cinema is one of very low risk. There is minimal processing of personal information and only basic information kept. The data is password protected and the biggest threat would come from hacking the database. As we hold minimal information, we assess the risk to be offset by the use of password protection and the management of the database will ensure the regular removal of unnecessary information.
- No financial information is stored.
- No gender or age information is stored.
- No preference information is stored.

6. Data Sharing

- We do not share data from the Membership Database.

7. Security measures

- We have a logon password for the computer and the membership database. This provides a two-step authentication process.
- A weekly back-up of the database is stored on the office computer where it is also password protected. The previous back-up is deleted. Breaches of security will be reported to the ICO within the required timescales.
- Further measures of security software, firewalls and encryption are under review.

8. Automated processing

- We use Facebook and Mail Chimp for automated processing and only email to previous customers who have a legitimate interest in receiving information from The Regal Cinema. There is an unsubscribe/opt out at each mailing.
- Facebook is used to profile audiences.
- We do not use profiling with Mail Chip.

9. Subject access requests

- Members can ask what information we hold about them and why
- By submitting a written request, Members will be shown a screen shot of their details on the database with other Members' names blacked-out for privacy

10. The right to be forgotten

- Members have the right to request to be forgotten. If they submit a written request they will be removed from the Membership Database within one month of the request.
- Members will be removed from all corresponding mail outs.

11. Privacy notices

The Regal Cinema aims to ensure that individuals are aware that their data is being processed, and that they understand:

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

To these ends the company has a privacy statement, setting out how data relating to these individuals is used by the company.

This privacy statement can be viewed at anytime upon request.

12. Ongoing documentation of measures to ensure compliance

Meeting the obligations of the GDPR to ensure compliance will be an ongoing process. The Regal Cinema details here the ongoing measures implemented to:

- 1) Maintain documentation/evidence of the privacy measures implemented and records of compliance
- 2) Regularly test the privacy measures implemented and maintain records of the testing and outcomes.
- 3) Use the results of testing, other audits, or metrics to demonstrate both existing and continuous compliance improvement efforts.
- 4) Keep records showing training of employees on privacy and data protection matters.

Although a formal evaluation of this policy will be conducted annually, this document should be considered a dynamic articulation of the organisations data management policy which is under constant revision.