Comar

Data Protection Policy

Table of Contents

Introduction

Comar needs to gather and use certain information about individuals.

These can include artists, audience, customers, suppliers, business contacts, employees, funders 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 protection policy ensures Comar:

- Complies with data protection law and good practice
- Protects the rights of staff, customers and partners
- Is open 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) became law in May 2018 and describes how organisations, including Comar, must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The General Data Protection Regulation is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes and only for the manner in which it was intended to be used
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than its intended purpose
6. Processed in accordance with the rights of the people the data is about
7. Be protected by technical and organisational security measures
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

Policy Scope

This policy applies to:

- All staff and volunteers of Comar
- All contractors, suppliers and people working on behalf of Comar

It applies to all data that Comar holds relating to identifiable individuals, even if that information technically falls outside of the General Data Protection Regulation. This can include:

- Names of individuals
- Postal addresses

- Email addresses
- Telephone numbers
- Racial or ethnic origin
- Political opinions
- Trade union membership
- Health data
- Sex life or sexual orientation
- Past or spent criminal convictions
- Any other information relating to individuals

The GDPR extends the definition of personal data (from the Data Protection Act 1998) to include:

- Genetic data
- Biometric data
- Location data
- Online Identifiers

Data Protection Risks

This policy helps to protect Comar from some very real data security risks, including:

- **Breaches of confidentiality**, for instance information being given out inappropriately
- **Failing to offer choice**, for instance all individuals should be fee to choose how Comar uses data relating to them
- **Reputational damage**, for instance Comar could suffer if hackers successfully gained access to sensitive data

Responsibilities

Everyone who works for or with Comar has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is collected, handled and processed in line with this policy and data protection principles. These people have specific areas of responsibility:

The **Board of Directors** is ultimately responsible for ensuring that Comar meets its legal obligations.

The **General Manager** (Data Protection Officer) 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
- Ensuring an audit of data collection and processing is carried out annually (Privacy Impact Assessment)
- Arranging data protection training and advice for the people covered by this policy
- Handling data protection questions from staff and anyone else covered by this policy
- Dealing with requests from individuals to see the data Comar holds about them (subject access request)
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data

The **Marketing (and IT) Officer** is responsible for:

- Maintaining a record of what personal data Comar holds
- Ensuring all It 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 Comar is considering using to store or process data, including cloud services
- Approving any data protection statements attached to communications such as emails and letters
- Addressing any data protection queries from journalists or media outlets
- 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 from their line managers
- Comar will provide training to all employees to help them understand their responsibilities when handling data
- Employees should keep all data secure by taking sensible precautions and following the guidelines below
- Strong passwords must be used and never shared
- Personal data should not be disclosed to unauthorised people either with the company or externally
- Data should be regularly reviewed and updated if it is found to be out of date and, if no longer required, should be disposed of
- Employees should request help from their line manager or the General Manager if they are unsure about any aspect of data protection

Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Marketing (IT) Officer.

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 for some reason:

- When not required, the paper or files should be kept in a locked cupboard or filing cabinet
- Employees should make sure paper and printouts are not left where unauthorised people could see them
- Data printouts should be shredded and disposed of securely when no longer required

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
- If data is stored on removable media, these should be kept locked away securely when not being used
- 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
- Data should be backed up frequently, with backups tested regularly
- Data should never be saved directly to laptops or other mobile devices
- All servers and computers containing data should be protected by an approved security software and a firewall

Data Use

Personal data is of no value to Comar unless we can make use of it, however this is when it is at greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended
- Personal data should not be shared informally, and never sent by email as this from of communication is not secure
- Data must be encrypted before being transferred electronically
- Personal data should never be transferred outside of the European Economic Area
- Employees should not save copies of personal data to their own computers but always access and update the central copy of any data
- Data breaches are to be reported to the Information Commissioner's Office (ICO) within 72 hours of discovery

Data Accuracy

The more important it is that the personal data is accurate, the greater the effort Comar should put into ensuring its accuracy. It is the responsibility if 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 additional unnecessary sets
- Staff should take every opportunity to ensure data is updated
- Comat will make it easy for data subjects to update the information Comar holds about them
- Data should be updated as inaccuracies are discovered, and removed if relevant
- It is the Marketing Officer's responsibility to ensure the marketing databases are checked every six months

Individual Rights

Individuals retain rights over our possession of their data to:

- Be informed about what we are doing with data
- Access their data
- Rectify their data where needed
- Erase their data ("right to be forgotten")

- Restrict processing
- Data portability (right to download their data and upload it to a different service provider)
- Object to our use of their data

Users may withdraw their consent at any time and do not have to give a reason.

Subject Access Requests

All individuals who are the subject of personal data held by Comar are entitled to:

- Confirmation that we are processing their data
- A copy of the personal data we hold on them
- Any other information we have in our possession about the subject, such as details of the data we have passed to third parties

If an individual contacts us requesting this information, this is called a subject access request (SAR). SARs from individuals should be made by email or letter, addressed to the General Manager, Karen Ray.

The relevant data will be provided within one month. The General Manager will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing Data for Other Reasons

In certain circumstances, the General Data Protection Regulation allows personal data to be disclosed to law enforcement agencies with the consent of the data subject.

Under these circumstances, Comar will disclose requested data. However, the General Manager will ensure the request is legitimate, seeking assistance from the board and from legal advisers if necessary.

Providing Information

Comar aims to ensure that individuals are aware that their data is being processed and that they understand how the data is being used and how to exercise their rights including their right to be forgotten.

To these ends, Comar has a privacy statement, setting out how data relating to individuals is used. This is available on request and is also on our website.

Review

We are committed to reviewing our policy and good practice annually.

This policy was last reviewed on ……..

Signed: ……

Alasdair McCrone