AUDIOACTIVE

DATA PROTECTION & GDPR
POLICY & PROCEDURE

Author:	**Policy Owner:**	**Reviewer:**	**Last Reviewed:**	**Next Review:**
Uschi Schomig	Uschi Schomig	Adam Joolia	March 2025	March 2027
Summary of Amendments:				

Key Messages

- The purpose of this document is to outline:
- How AudioActive will ensure compliance with the UK GDPR and Data Protection Act 2018.
- Explain the roles and responsibilities relevant to internal compliance.
- How compliance with this policy will be monitored.

This policy applies to all AudioActive employees, freelancers, volunteers & beneficiaries.

AUDIOACTIVE

CONTENTS

AUDIOACTIVE

Introduction

This policy provides a framework for ensuring that AudioActive meets its obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 18).

AudioActive complies with data protection legislation guided by the six data protection principles. In summary, they require that personal data is:

- processed lawfully, fairly and in a transparent manner.
- used only for limited, specified stated purposes and not used or disclosed in any way incompatible with those purposes.
- adequate, relevant and limited to what is necessary.
- accurate and, where necessary, up to date.
- not kept for longer than necessary.
- kept safe and secure.

In addition, the accountability principle requires us to be able to evidence our compliance with the above six principles and make sure that we do not put individuals at risk because of processing their personal data. Failure to do so, can result in breach of legislation, reputational damage, or financial implications due to fines. To meet our obligations, we put in place appropriate and effective measures to make sure we comply with data protection law.

Our staff have access to a number of policies, operational procedures and guidance to give them appropriate direction on the application of the data protection legislation, this includes overarching documents such as;

- Archiving & Retention Schedule
- Information Management Policy
- Information Sharing Protocol & Agreements
- Confidentiality Agreement
- Register of Processing Activities (RoPA)
- Privacy Notices
- Complaints Procedure

AUDIOACTIVE

Information Covered by Data Protection Legislation

The UK GDPR definition of "personal data" includes any information relating to an identified or identifiable natural living person.

Pseudonymised personal data is covered by the legislation, however anonymised data is not regulated by the UK GDPR or DPA 18, providing the anonymisation has not been done in a reversible way.

Some personal data is more sensitive and is afforded more protection, this is information related to:

- Race or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric ID data;
- Health data;
- Sexual life and/or sexual orientation; and
- Criminal data (convictions and offences)

Our Commitment

AudioActive is committed to transparent, lawful, and fair proportionate processing of personal data. This includes all personal data we process about staff, volunteers, beneficiaries, or those who work or interact with us.

Privacy notices
We publish a detailed privacy notice on our website. This outlines data subjects' rights, along with the what, why and how of our data processing. We also publish a more accessible, simplified version suitable for children and young people.

Training
All staff are required to undertake an online data protection training module during their induction. We provide annual in-house training for all staff on information governance and security.

Breaches
We consider personal data breach incidents and have a reporting procedure that is communicated to all staff. We assess whether we need to report breaches to the ICO as the Regulator of DPA. We take appropriate action to make data subjects aware, if needed.

Information Rights
We have a clear process to handle subject access requests and other information rights requests, and will respond within the timeframes set out by regulations.

Data Protection by Design and Default
We have a procedure to assess processing of personal data perceived to be high risk, and carry out a Data Protection Impact Assessment (DPIA) where required. We ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Security
Systems and processes are regularly reviewed to look at access and to identify and mitigate risk. We undertake monthly data back-ups.

Data Retention and Deletion
Our archiving & retention procedure (Annex B) shall consider what data should/must be retained, for how long, and why; in line with our business requirements and legal obligations.

Record of Processing Activities (RoPA)
We record our processing activities, legal bases and processing of special category data in a document which is regularly reviewed and updated, where necessary.

Policies and Procedures
We produce policies and guidance on information management and compliance that we communicate to staff.

Monitoring

Compliance with this policy will be monitored by the DPO and governance team listed below.

AUDIOACTIVE

Roles and Responsibilities

Data Protection Officer (DPO) - The DPO is primarily responsible for advising on and assessing our compliance with the DPA and UK GDPR, and making recommendations to improve compliance. AudioActive's DPO is Uschi Schomig, and she can be contacted on data@audioactive.org.uk.

Information Asset Owners (IOAs) - IAOs have local responsibility for data protection compliance in their area/directorate. This includes any Manager who makes decisions around day to day use of data.

Senior Information Asset Owner - CEO, Adam Joolia, holds overall responsibility for data protection compliance.

Senior Information Risk Owner (SIRO) - A member of the Board of Trustees with overall corporate responsibility for GDPR compliance. Our SIRO is Board Chair and Non-Executive Director, Arjo Ghosh.

Annex A - Glossary

Data Subject - A data subject is an identifiable individual person about whom the Charity holds personal data.

Personal Data - Any information relating to an identifiable living individual who can be identified from that data or from that data and other data. This includes not just being identified by name but also by any other identifier such as ID number, location data or online identifier, or being singled out by any factors specific to the physical, physiological, genetic, mental, cultural or social identity of the individual.

Special Category Personal Data - Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying an individual, data concerning health or data concerning an individual's sex life or sexual orientation.

Data Controller - The organisation (or individual) which, either alone or jointly with another organisation (or individual) decides why and how to process personal data. The Controller is responsible for compliance with the DPA and GDPR.

Processing - Anything that is done with personal data; including collection, storage, use, disclosure, and deletion.

Data Processor - Any person or organisation contracted to handle data on behalf of a Data Controller. Examples of data processors in use by AudioActive can be found in our Privacy Notice.

Personal Data Breach - A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed.

Pseudonymisation - The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Lawful bases - In order to lawfully process personal data, one or more legal bases must apply. The lawful bases for processing are set out in Article 6 of the UK GDPR:

- **Consent** - the data subject has given consent to the processing of his or her data for one or more specific purposes
- **Contract** - processing is necessary for the performance of a contract
- Legal obligation - processing is necessary for compliance with a legal obligation to which the controller is subject
- **Vital interests** - processing is necessary in order to protect the vital interests of the data subject or of another natural person
- **Public task** - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- **Legitimate interests** - processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

AUDIOACTIVE

Annex B - Archiving & Retention of Documents Procedure

Table 1 - Statutory Retention Periods

Record Type	Statutory Retention Period	Statutory Authority
Accident Books,accident records/reports	3 years from the date of the last entry (or, if the accident involves a child/ young adult, then until that person reaches the age of 21)	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) (SI 1995/3163) as amended, and Limitation Act 1980
Accounting Records	3 years for private companies, 6 years for public limited companies	Section 221 of the Companies Act 1985 as modified by the Companies Acts 1989 and 2006
1st Aid Training	6 years after employment	Health and Safety (First Aid) Regulations 1981
Fire warden training	6 years after employment	Fire Precautions (Workplace) Regulations 1997
Health and Safety representatives and employees' training	5 years after employment	Health and Safety (Consultation with Employees) Regulations 1996; Health and Safety Information for Employees Regulations 1989
Income tax and NI returns, income tax records and correspondence with HMRC	Not less than 3 years after the end of the financial year to which they relate	The Income Tax (Employments) Regulations 1993 (SI 1993/744) as amended,

		for example by The Income Tax (Employments) (Amendment No. 6) Regulations 1996 (SI 1996/2631)

Record Type	Statutory Retention Period	Statutory Authority
National minimum wage records	3 years after the end of the pay reference period following the one that the records cover	National Minimum Wage Act 1998
Payroll wage/salary records (also overtime, bonuses, expenses)	6 years from the end of the tax year to which they relate	Taxes Management Act 1970
Records relating to children and young adults	until the child/young adult reaches the age of 21	Limitation Act 1980
Statutory Maternity Pay records, calculations, certificates (Mat B1s) or other medical evidence (also shared parental, paternity and adoption pay records)	3 years after the end of the tax year in which the maternity period ends	The Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960) as amended, Maternity & Parental Leave Regulations 1999
Subject access request	1 year following completion of the request	Data Protection Act 2018.
Whistleblowing documents	6 months following the outcome (if a substantiated	Public Interest disclosure Act 1998 and

	investigation). If unsubstantiated, personal data should be removed immediately	recommended IAPP practice
Working time records including overtime, annual holiday, jury service, time off for dependents, etc	2 years from date on which they were made	The Working Time Regulations 1998 (SI 1998/1833)

Table 2-Recommended Retention Periods

Record Type	Recommended Retention Period
HR Records	
Assessments under health and safety regulations and records of consultations with safety representatives and committees	Permanently
CCTV footage	CCTV footage may be relevant to a disciplinary matter or unfair dismissal claim. Recommended Information Commissioner's Office (ICO) retention practice is 6 months following the outcome of any formal decision or appeal
Flexible working requests	18 months following any appeal. This is because a further request cannot be made for 12 months following a request plus allowing for a 6 month tribunal limitation period on top
Inland Revenue/HMRC approvals	Permanently

Parental leave	18 years from the birth of the child
Pension records	12 years after the benefit ceases
Personnel files and training records (including formal disciplinary records and working time records)	6 years after employment ceases but note that it may be unreasonable to refer to expired warnings after two years have elapsed
Personnel files and training records (including formal disciplinary records and working time records)	6 years after employment ceases but note that it may be unreasonable to refer to expired warnings after two years have elapsed

Table 2-Recommended Retention Periods continued

Record Type	Recommended Retention Period
Recruitment application forms and interview notes (for unsuccessful candidates)	6 months to a year. Because of the time limits in the various discrimination Acts, minimum retention periods for records relating to advertising of vacancies and job applications should be at least 6 months
Redundancy details, calculations of payments, refunds, notification to the Secretary of State	6 years from the date of redundancy
Right to work in the UK checks	Home Office recommended practice is 2 years after employment ends
Statutory Sick Pay records, calculations, certificates, self-certificates, occupational health reports	The Statutory Sick Pay (Maintenance of Records) (Revocation) Regulations 2014 (SI 2014/55) abolished the former obligation on employers to keep these records. Although there is no longer a specific statutory retention period,

	employers must still keep sickness records to best suit their business needs. It's advisable to keep records for at least 6 months after the end of the period of sick leave in case of a disability discrimination claim. However, if there's a personal injury claim, the limitation is 3 years. If there's a contractual claim for breach of an employment contract, it may be safer to keep records for 6 years after the employment ceases.
Termination of employment, for example early retirement, severance or death in service	At least 6 years
Terms and conditions including offers, written particulars, and variations	Review 6 years after employment ceases or the terms are superseded
Trustees' minutes	Permanently