Title:	**Data Protection (Compliance Management) Policy**
Code:	**WBDPCM-01**
Published:	**October 2023**
Review date:	
Approved by:	**SMT**
Policy owner:	**Victoria Collis**

Contents

1 Policy Scope, Background & Objectives

1.1 Scope

This Data Protection Policy sets out the organisation's commitment and approach to data protection and provides a clear frame of reference for employees to determine the organisation's standards, aims, and ideals in respect of data protection compliance.

The policy's objectives are:

- To provide a clear frame of reference for employees to determine the organisation's standards, aims, and ideals in respect of data protection compliance;
- To provide information to data subjects, data processors, and the regulatory authorities about how the organisation approaches data protection compliance.

Unless otherwise stated this document applies to all personal data processed by WaterBear. It applies to any natural or legal person who process personal data for or on behalf of WaterBear including: employees, volunteers, casual and temporary employees, directors and officers, external organisations employed as processors and any external organisations or individuals with whom WaterBear shares or discloses personal data. It also applies where WaterBear is a joint controller or where relevant, acts as a processor for another controller.

1.2 Background

The processing of personal data in the United Kingdom is regulated by law. The principle statutory instrument setting out the legal obligations of those handling personal data, the rights of data subjects whose data is processed, and the offences, penalties and remedies is the Data Protection Act 2018 ("the Act"). Other laws inter-relate with the Act and the GDPR including but not limited to the Privacy and Electronic Communications Regulations (2003), the Freedom of Information Act (2000). These laws are collectively referred to in this Policy as Data Protection Legislation.

Additionally, various guidelines, codes or practice, case law and other information relating to data protection must be considered by the organisation.

The Data Protection Legislation sets out legal responsibilities on all organisations processing personal data and provide for rights in the law conveyed on the people whose data are being processed.

This Policy is a public statement describing the organisation's approach to complying with it's legal responsibilities in the Data Protection legislation and how it enables individual rights to be upheld and exercised.

Penalties can be imposed on organisations processing personal data including fines of up to €20,000,000 or 4% of prior year global annual turnover whichever is the greater. There are a number of criminal offences set out in the Data Protection Legislation and individuals can be held accountable and be sentenced by the courts for offences under the Data Protection Legislation.

The reader should refer to the Glossary to ensure that they understand the terms used in this Policy.

Related and connected laws:

- The Data Protection Act 2018
- The General Data Protection Regulation
- The Common Law Duty of Confidentiality
- The Freedom of Information Act 2000
- Data Retention and Investigatory Powers Act 2014
- Privacy and Electronic Communications Regulations (PECR) 2003
- Computer Misuse Act 1990
- Human Rights Act 1998

1.3 Definitions

The terms used in this framework have the meanings attributed to them in the General Data Protection Regulation and the Data Protection Act 2018. Principle terms are also defined in the Glossary of this framework.

2 Policy Statement

WaterBear is committed to compliance with all relevant Data Protection Legislation and will formally delegate appropriate powers and responsibilities to its personnel to ensure that it is fully able to comply with the Data Protection Legislation and its own defined standards in the field of data protection and information governance.

The organisation will maintain a suite of policy documents setting out how it intends to implement management controls sufficient to ensure legal compliance and will ensure that these documents are reviewed periodically to:

a) test their adequacy in meeting the legal standards as they change over time, and
b) to test the organisation's compliance with them.

The organisation will ensure that all relevant personnel and/or other persons it commissions to process personal data on its behalf, either directly or indirectly, have received appropriate and sufficient training in the application of the organisation's policies.

The management will ensure that sufficient and appropriate resources are available to ensure that it meets both its legal obligations in respect of Data Protection Legislation and the standards that it sets through its policies.

The management will ensure that the organisation works within the 7 Key Principles and that it will implement sufficient controls to ensure that it is able to demonstrate compliance with the Data Protection Legislation including the keeping of sufficient records of data processing activities, risk assessments and decisions relating to data processing activities.

The organisation will uphold the rights and freedoms of people conferred on them by the Data Protection Legislation. It will ensure that those rights and freedoms are appropriately considered in the decisions it takes which may affect people and will ensure that it has sufficient controls in place to assist people who wish to exercise their rights.

This policy applies to all the organisation's activities or operations which involve the processing of personal data.

This policy applies to anyone who is engaged to process personal data for or on behalf of the organisation including: employees, volunteers, casual and temporary staff, directors and officers, and third parties such as sub-contractors and suppliers, and anyone who the organisation shares or discloses personal data with/to.

3. Responsibilities

3.1 Data controller

WaterBear is the legal data controller under the Data Protection Legislation.

3.2 Management and supervisory staff.

The CEO is the accountable officer responsible for the management of the Organisation and ensuring appropriate mechanisms are in place to support service delivery and continuity. Protecting data and thus maintaining confidentiality is pivotal to the Organisation being able to operate. Each Director, in their respective areas of responsibility, must ensure that all staff members are aware of this policy, other relevant policies and procedures, and their responsibilities concerning the processing of personal data. Each Director must ensure this policy is adhered to. Managers and supervisory staff are responsible for ensuring that all data processing operations under their control or sphere of responsibility or commissioned by them are undertaken in compliance with this policy and other relevant data protection policies. They are responsible for ensuring that anyone processing data is sufficiently aware of this policy and how it applies to their job role and sufficiently trained to carry out their duties in compliance with this policy.

3.3 Senior Information Risk Officer (SIRO)

The organisation has appointed a SIRO to lead and implement the information governance risk assessment programme and advise the Board on the effectiveness of information risk management across the Organisation.

WaterBear's Senior Information Risk Officer: **Victoria Collis**

3.4 Data Protection Officer

The Data Protection Officer is responsible for providing the policies, guidance and training needed to ensure the Organisation is both compliant with Data Protection Legislation and risk assessed. They will monitor and report to the GDPR Steering Committee in respect of compliance with this policy, investigate any breaches, and maintain suitable records of processing activities. They may co-opt other individuals to assist with the management of data protection obligations. The DPO is responsible for monitoring the evolution of the Data Protection Legislation, case law, guidance, and codes of practice and incorporating relevant changes into the Organisation's policy.

WaterBear's Data Protection Officer: Elliott Groves

3.5 Information Asset Owners

Information assets are identified in an Information Asset Register which is maintained by Information Asset Owners. The Board of Directors assigns an Information Asset Owner to each information asset. The Information Asset Owner has primary operational responsibility for compliance with data protection legislation and good practice in respect of assigned information assets. Information Asset Owners are senior individuals responsible for a discrete business area. Their role is to understand what personal data are used in their business area and how it is used, who has access to it and why. As a result, they can understand and address risks to the data and the organisation within the Information Governance Framework.

Where the nature of WaterBear's business is such that personal data are processed as part of a single business process across a number of separate hierarchical business units then, responsibility for the business process may be assigned to an Information Asset Owner.

As senior managers, Information Asset Officers may delegate day-to-day responsibility for compliance within their management hierarchies, subject to other HR policies and ensuring that all staff are appropriately trained.

3.6 GDPR Steering Committee

The objective of the GDPR Steering Committee is to ensure compliance with the requirements and principles outlined in the GDPR and other related data protection laws.

The committee will provide guidance, oversight and strategic direction in managing personal data while considering the risks of the processing activities.

3.7 Operational Responsibility

WaterBear have operational responsibility for compliance with data protection policies and best practice in relation to HR policies and procedures including recruitment and retention. In liaison with the Data Protection Officer, WaterBear are responsible through the staff performance

management framework for ensuring that training needs analysis is undertaken in respect of all posts and that appropriate data protection awareness and training is provided, measured and reported.

3.8 IT & Security

WaterBear has operational responsibility for compliance with data protection legislation and best practice for information security in respect of WaterBear's IT estate.

3.9 Employees, volunteers, casual/temporary workers, directors and officers etc.

Anyone who is directly engaged by the organisation to undertake data processing activities including but not limited to employees, volunteers, casual/temporary workers, directors and officers etc. involved in the receipt, handling or communication of personal data must adhere to this policy. Anyone who is not confident in or has concerns about data handling practices that they are undertaking, or witnessing should contact the Data Protection Officer. Individuals are expected to complete appropriate training from time to time.

Everyone within the Organisation has a duty to respect data subjects' rights to confidentiality.

Disciplinary action and / or penalties could be imposed on staff for non-compliance with relevant policies and legislation.

3.10 Partner & Third-Party Responsibilities

Any Third Party or Organisation that is commissioned to process data or receives data from the organisation, or is able to access any personal data must enter into a legally enforceable agreement

with the organisation the nature of which will be determined by the level of involvement with the data that is held/shared/accessed.

4 Policy Detail

4.1 Data Protection Officer

WaterBear has determined that it is required to designate a Data Protection Officer due to the regular of monitoring of data subjects on a large scale and the regular processing of personal data.

4.2 Fair Lawful and Transparent processing

The processing of all personal data by the organisation will only be undertaken in a fair, lawful and transparent manner meaning:

Fairness – no data collection activities will be undertaken or commissioned without an appropriate privacy notice being provided to the person from whom data are being collected and to the people who the data are about if personal data are collected from sources other than the data subject. All privacy information and any changes to privacy information will be reviewed by the DPO.

Lawfulness – no data collection activities will be undertaken or commissioned without there being a lawful ground for the data processing activities intended to be applied to the personal data. The DPO is responsible for determining the lawful grounds for processing. Where the lawful grounds are consent, the consent policy will apply. Where the lawful grounds are legitimate interests a legitimate interests assessment (LIA) will be undertaken and documented. Where the lawful grounds are a task carried out in the public interest or in the exercise of official authority vested in the organisation, a public interests assessment (PIA) will be undertaken and documented. Where the lawful grounds are a legal obligation, the relevant legislation shall be cited and appropriately documented. The information process owner is responsible for ensuring that there are lawful grounds for all data processing activities that fall under their sphere of control, that the consent

policy is adhered to and a LIA/PIA is properly undertaken where necessary. The DPO will provide advice regarding lawful processing conditions.

Transparency – the organisation will endeavour to provide sufficient information about how personal data are being processed to enable sufficient transparency about its handling of personal data. The DPO is tasked with periodically reviewing the apparent transparency.

4.3 Data processing purposes

Personal data will only be collected, created or otherwise obtained for specific, explicit and legitimate purposes and should be reviewed by the DPO. The organisation shall maintain a register of data processing activities and their purpose.

Data process owners are responsible for ensuring that all the data processing activities that they undertake and/or commission and are reviewed by the DPO.

4.4 Data minimisation

The organisation will strive to use a minimum of personal data in its data processing activities and will periodically review the relevance of the information that is collects. Data process owners are responsible for ensuring that no unnecessary, irrelevant or unjustifiable personal data are collected or created either directly or indirectly through the data processing activities they are responsible for and/or engage in. The DPO will provide advice regarding the justification of personal data collected or created.

4.5 Data accuracy

WaterBear recognise that the accuracy of data is important, and that some data is more important to keep up to date than others. The organisation will use its reasonable endeavours to maintain data as accurate and up to date as possible, in particular data which would have a detrimental impact on data subjects if it were inaccurate or out-of-date. Data process owners are responsible for ensuring that personal data they have collected or created either directly or indirectly through the data

processing activities they are responsible for and/or engage in are maintained accurate and up-to-date and that personal data whose accuracy cannot reasonably be assumed to be accurate and up-to-date are treated appropriately through erasure or anonymisation. The DPO will provide advice regarding data accuracy.

4.6 Data retention

The organisation will ensure that it does not retain personal data for any longer than is necessary for the purposes for which they were collected and will apply appropriate measures at the end of data's useful life such as erasure or anonymization. Data process owners will be responsible for determining the retention period for personal data under control or sphere of influence and the organisation will maintain a data retention schedule setting out approved retention periods and end of life treatment. The DPO must review all retention periods for personal data. Because data retention is a vitally important issue as both the over-retention and under-retention of personal data could have a detrimental impact on both the data subject and the organisation the DPO will undertake data retention audits.

4.7 Information security

The organisation will ensure that any personal data that it processes or commissions the processing of is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. Network Security will be maintained setting out specific policies in relation to maintaining personal data secure, confidential, available and with integrity. The DPO is authorised to challenge Network Security and is required to report any concerns to the GDPR Steering Committee.

4.8 Children's data

Special measures will be taken by the organisation if it processes personal data relating to children under the age of 13 including the nature of privacy information provided and approach to

information rights requests. These special measures will be set out in a policy relating to children's data.

4.9 Personal data relating to criminal convictions and offences

Where the organisation is processing personal data relating to criminal convictions and offences it shall implement suitable measures including a policy document that satisfies the requirements of the Data Protection Act 2018 Schedule 1 Parts 3 and 4.

4.10 Special categories of personal data

The organisation shall not process special categories of personal data unless it has documented the lawful grounds for such processing and maintains periodic review of the necessity to processing the special categories of personal data.

The organisation shall adopt the definition of special categories of personal data from the GDPR which shall be 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 a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

4.11 Consent

The organisation will interpret consent to be as defined in the GDPR and that any consent shall not be valid unless:

- there is a genuine choice;
- it has been explicitly and freely given, and represents a specific, informed and unambiguous indication of the data subject's wishes that signifies agreement to the processing of personal data relating to them;
- the consent was given through statement made by the data subject or by a clear affirmative action undertaken by them;

- the organisation can demonstrate that the data subject has been fully informed about the data processing to which they have consented and is able to prove that it has obtained valid consent lawfully;
- a mechanism is provided to data subjects to enable them to withdraw consent and which makes the withdrawal of consent in effect as easy as it was to give and that the data subject has been informed about how to exercise their right to withdraw consent;

The organisation recognises that consent may be rendered invalid in the event that any of the above points cannot be verified or if there is an imbalance of power between the data controller and the data subject.

The organisation recognises that consent cannot be considered to be forever and will determine a consent refresh period for every instance where consent is the lawful condition for processing.

4.12 Record keeping and accountability

In order to fulfil its responsibility to be able to demonstrate compliance with Data Protection Legislation, as well as in support the policy on transparency, the organisation will maintain records of the processing activities that it controls, undertakes or otherwise commissions as required by the Data Protection Legislation and specifically those required in Article 30 of the GDPR.

4.13 Information rights

The organisation recognises the legal rights of those whose data it is processing or intends to process and will ensure that appropriate information is provided to them advising them of their rights, and that policies and procedures are maintained to ensure that the organisation is able to recognise information rights requests and handle them appropriately when they are exercised. These rights include:

- Right to information about data processing operations
- Right of access to personal data
- Right to portability of personal data
- Right of rectification of personal data

- Right of erasure of personal data
- Right to restriction of processing
- Right to object to direct marketing
- Right to object to data processing operations under some circumstances
- Right not to be subject to decisions made by automated processing under some circumstances
- Right of complaint about the organisation's processing of personal data and the right to a judicial remedy and compensation

4.14 Personal Data Breaches

The organisation will maintain a Data Breach Reporting Procedure and will ensure that all employees and those with access to personal data are aware of it and this breach reporting policy. All employees and individuals with access to personal data for which the organisation is either data controller or processor must report all personal data breaches to an appropriate individual as set out in the Data Breach Reporting Procedure as soon as they become aware of the breach. The organisation will log all personal data breaches and will investigate each incident without delay. Appropriate remedial action will be taken as soon as possible to isolate and contain the breach, evaluate and minimise its impact, and to recover from the effects of the breach. Data protection near misses will also be recorded and investigated in the same manner as data protection breaches. The breach reporting procedure will set out responsibilities, decision-making criteria and timescales for notifying data subjects and the Information Commissioner's Office (ICO) about a personal data breach.

4.15 Data Processors

The organisation reserves the right to contract out data processing activities or operations involving the processing of personal data in the interests of business efficiency and effectiveness. No third-party data processors will be appointed who are unable to provide satisfactory assurances that they will handle personal data in accordance with the Data Protection Legislation. People wishing to appoint a data processor will ensure that appropriate due diligence is undertaken on the proposed data processor in the field of information governance and data protection compliance prior to their appointment. The DPO will provide advice and guidance in respect of this. A written agreement will

be implemented between the Organisation and the data processor which at least meets the requirements of the Data Protection Legislation. WaterBear will maintain a register of such agreements/arrangements. The data processor agreement will specify what is to happen to personal data upon termination of the data processing agreement.

No employee is permitted to commission or appoint a third party to process data on behalf of the organisation without adhering to this policy.

4.16 The organisation as a data processor

Where the organisation acts as a data processor it shall ensure it retains records of processing which record at least the information required under Article 30(2) of the GDPR for each controller it acts on behalf of. The organisation shall ensure that it has an appropriate agreement in place with each data controller and shall ensure that its employees, volunteers, staff and contractors, receive appropriate training to enable them to ensure compliance with the instructions and contractual terms of each data controller.

4.17 Data sharing, disclosure and transfer

The organisation will only share personal data with or otherwise disclose personal data to other organisations and third parties where there is a legal basis for doing so and the data sharing is necessary for specified purposes. No data sharing or disclosure is permitted to occur without a suitable legally enforceable agreement satisfying the requirements for such agreements as set out in the Data Protection Legislation being in place. Data sharing agreements must be approved by the DPO who will maintain a register of all such agreements.

Appropriate risk assessments will be undertaken prior to any data sharing taking place on those with whom we intend to share personal data. This policy extends to appointing others to process personal data on our behalf, sharing personal data with organisations, and providing information to ad hoc requests for information such as those which may be received from the police and other authorities.

The organisation will provide information to all employees setting out safe and approved methods of transferring personal data to recipients. Employees are required to use only approved methods of data transfers. Disciplinary action will be taken against employees who fail to observe the data transfer policy and use unsafe and insecure methods of data transfer unless such methods have been approved in writing.

4.18 Internationalisation of personal data

The organisation will neither transfer nor process nor will it permit personal data to be transferred or processed outside the United Kingdom without the conditions laid down in the Data Protection Legislation being met to ensure that the level of protection of personal data are not undermined. Any transfer or processing of personal data that the organisation undertakes or commissions whether directly or indirectly must be approved by the Board of Directors, and reviewed by the DPO, and may only take place if one of the following is satisfied:

- The territory into which the data are being transferred is one approved by the UK's Information Commissioner;
- The territory into which the data are being transferred is within the European Economic Area;
- The territory into which the data are being transferred has an adequacy decision issued by the European Commission;
- The transfer is to the United States of America and the recipient is registered under the EU/US Privacy Shield scheme;
- The transfer is made under the unaltered terms of the standard contractual clauses issued by the European Commission for such purposes;
- The transfer is made under the provision of binding corporate rules which have been approved and certified by the European Commission;
- The transfer is made in accordance with one of the exceptions set out in the Data Protection Legislation.

4.19 Risk assessment

The organisation will embrace the principles and foster a culture of privacy by design and by default. It will maintain a policy requiring data protection impact assessments (DPIA) to be undertaken and documented and ensure that appropriate resources are available to advise on DPIAs. A risk register will be maintained of data protection compliance risks that have been identified by the organisation and for its periodic review.

4.20 Training and awareness

The Organisation will ensure that all those who it engages to process personal data either directly or indirectly are provided with appropriate training in the application of this and other data protection policies and procedures and in their data protection responsibilities. It will also undertake data protection awareness raising activities from time to time to keep data protection front of mind. All training and awareness raising activities will be logged. Refresher training will be provided periodically.

4.21 Continuous Improvement, audit and compliance checking

The organisation will undertake periodic compliance checks to test whether its policies and procedures are being adhered to and to test the effectiveness of its control measures. Corrective action will be required where no-conformance is found. Records will be kept of all such audits and compliance checks including corrective action requests raised. Disciplinary action will be taken against individuals who fail to act upon the reasonable corrective action requests properly formulated and raised through data protection audits. The GDPR Steering Committee will be provided with a summary of audit findings periodically.

4.22 Data protection by design and by default

The organisation shall strive to foster a culture of data protection by design and by default in all its data processing activities. It shall ensure that measures are in place to encourage all those involved in data processing activities to adopt a model of continuous improvement to the technical and organisational measures that implement the data protection principles and safeguards into

processing activities. The organisation shall strive to ensure that by default, only personal data which are necessary for each specific purpose of the processing are processed and that the extent of the processing, period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

5 Glossary

Data Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

Data Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

Data subject any living individual who is the subject of personal data held by an organisation;

Data Process Owner The person responsible for the instigation or on-going maintenance of a data process or data processing operation;

Personal data means any information relating to an identified or identifiable living individual;

Identifiable living individual means a living individual who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data or an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual;

Special Categories means any personal data revealing racial or ethnic origin, political

of Personal Data opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation;

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Information Incident means an identified occurrence or weakness indicating a possible breach of information security or failure of safeguards, or a previously unknown situation which may be relevant to the security of information;

Personal Data Breach means 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;

Risk The chance of something happening, which will have an impact upon objectives. It is measured in terms of consequence and likelihood;

Risk Management The culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects;

Senior Information an Executive Director or member of the Senior Management Board

Risk Owner (SIRO) with overall responsibility for the Organisation's information risk strategy;

Corporate Data relates to any sensitive corporate information including meeting schedules, agendas and minutes of meetings; financial accounts; contracts; and organisational policies and procedures.

Recipient means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

Third party Means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

Profiling Is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual;

Consent means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data;


WATER
BEAR
The College of Music