Data Protection Policy

MOMENTUM

Version	1.3
First publication date	8th April 2019
Current version publication date	22nd December 2022
Next review	December 2023

1. Introduction

1.1 Purpose

1.2 Data protection legislation, including the General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018 applies to all information relating to an identified or identifiable living individual. This is defined as personal data within data protection legislation.

1.3 Momentum takes the protection of all personal information extremely seriously and is committed to a policy of protecting the rights and freedoms of individuals with respect to the processing of their personal information.

1.4 This policy falls under the remit of the Company's Information Governance Framework and as such should be read and implemented alongside the other policies and procedures in this framework.

1.5 Scope

1.6 Momentum holds and processes information about its current, past and prospective employees, clients, and a large volume of patient data all of whom are defined as data subjects within data protection legislation.

1.7 Momentum Data processes personal information for a variety of reasons including:

- 1.7.1 Medical research
- 1.7.2 Quality improvement studies
- 1.7.3 Clinical audit
- 1.7.4 Feasibility analyses
- 1.7.5 Business administration and management
- 1.7.6 Fundraising and Marketing

1.8 Definitions

1.9 Chief Information Officer (CIO); Momentum Data's responsible officer for information security compliance, Andrew McGovern.

1.10 Information Governance Officer (IGO); Momentum Data's responsible officer for information governance, Joseph Babbage.

1.11 Data Subject - a natural person whose personal data is processed by Momentum Data or by an appointed data processor.

1.12 Data Controller - the entity that determines the purposes, conditions and means of the processing of personal data.

2. Principles

2.1 Anyone who processes personal information within Momentum must comply with the principles of data protection. The Principles define how data can be legally processed. Processing means any operation which is performed on personal data or sets of personal data, by automated or manual means such as collecting, recording, organising, storing, adapting, altering, consulting, using, disclosing, combining, restricting, erasing or destroying.

2.2 The principles of data protection state that personal data shall be:

2.2.1 processed lawfully, fairly and in a transparent manner in relation to the data subject;

2.2.2 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 purposes or statistical purposes shall not be considered to be incompatible with the initial purposes (although certain other safeguards must be in place as defined within the GDPR);

2.2.3 adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

2.2.4 accurate and, where necessary, kept up to date;

2.2.5 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 when processed only for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of appropriate measures to protect the rights and freedoms of data subjects;

2.2.6 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.

3. Roles and Responsibilities

3.1 Momentum shall be responsible for, and be able to demonstrate compliance with data protection legislation.

3.2 Momentum, as data controller, is responsible overall for demonstrating compliance with data protection legislation and meeting the accountability and transparency obligations within the legislation.

3.3 All company leads and managers have a responsibility to ensure compliance with data protection legislation and this policy, and to develop and encourage good information handling practices within their areas of responsibility.

3.4 All staff have a responsibility to ensure they process personal data in accordance with the data protection principles and other requirements of data protection legislation.

3.5 Where required the CIO or IGO will oversee periodic audits to ensure compliance with this policy.

3.5.1 Specific audits to be carried out annually are to cover file sharing and self-report questionnaires covering understanding of the processes.

3.5.2 Following these audits, any problem areas and employees not following procedure will be highlighted by the IGO. Necessary action plans will be created to rectify these issues, with reasonable timelines. If required, the IGO will escalate corrective actions to the CIO / DPO.

4. Procedures

4.1 Information Asset Owners

4.1.1 Each major information asset held by Momentum containing personal data will have an assigned member of staff to be the named Information Asset Owner for that asset.

4.1.2 An Information Asset Owner will be a member of staff who manages an information or data asset and has the power to make decisions about how that information is managed.

4.1.3 Information Asset Owners will work with the CIO to disseminate guidance and information relating to data protection and good information handling practices, as well as managing breach reporting within their area and maintaining the appropriate registers to demonstrate accountability in relation to data protection.

4.1.3.1 All data incidents should be reported following the Company's Procedure for Reporting Data Incidents which is available in the Staff Handbook.

4.1.3.2 The Information Asset Register is stored under Nextcloud\Information Governance\Information Assets Register. This includes the Record Retention Schedule.

4.2 Record of processing

4.2.1 Information Asset Owners will be responsible for recording data assets within the company's data asset register and for maintaining this register.

4.2.2 Formal permission from the CIO is required before the addition of any new asset to the company's systems.

4.2.3 The Record of Processing Activities is stored under Nextcloud\Information Governance\Information Assets Register.

4.3 Privacy Impact Assessments

4.3.1 All major data processing activities, especially new processing of personal data or adaptations of existing methods of processing, will be assessed to ensure that the proposed processing complies with the requirements of data protection.

4.4 Data transfer and storage

4.4.1 All data transfer and storage must be performed in accordance with the company's Standard Operating Procedure for Data transfer and Storage which is available to all staff via the Staff Handbook.

4.4.2 Any breach of the standard operating procedures should be reported immediately to the CIO and the Information Asset Owner.

4.4.3 Any documents saved to Slack are automatically deleted as per Slack's internal policies.

4.4.4 Documents stored on Nextcloud are deleted in accordance with the company's Standard Operating Procedure for Data Transfer and Storage, which is available to all staff via the Staff Handbook.

4.5 Reporting of data incidents

4.5.1 All data incidents must be reported in accordance with the company's standard operating procedure for reporting data incidents which is available to all staff via the staff handbook.

5. Data subject rights

5.1 Momentum will comply with all data subject rights, as appropriate in relation to the processing it undertakes.

5.2 These rights are:

5.2.1 Transparency of processing

5.2.2 Right of access to personal data

5.2.3 Right of rectification of inaccurate personal data

5.2.4 Right of erasure

5.2.5 Right to restriction of processing

5.2.6 Right to data portability

5.2.7 Right to object to processing where it is processed in the following way:

5.2.7.1 for direct marketing purposes

5.2.7.2 for scientific/historical/research/statistical purposes

5.2.7.3 based on legitimate interest grounds

5.2.8 necessary for the performance of a task carried out in the public interest

5.2.9 Right to object to automated individual decision making, including profiling

6. Transparency of processing

6.1 Wherever personal data is collected for a new purpose, the Information Asset Owner responsible for that data will ensure a Privacy Notice is created and shared with data subjects if applicable.

6.2 This Privacy Notice will include:

6.2.1 Name of data controller and contact details

6.2.2 Contact details of the CIO

6.2.3 Purposes of processing the data

6.2.4 Legal basis of processing

6.2.5 Transfers outside the EU

6.2.6 Length of time for which data will be retained

6.2.7 Data subject rights in relation to the data

6.2.8 Recipients of the data

6.2.9 Statutory or contractual requirements to provide the data

6.2.10 Any automated decision-making including profiling

6.2.11 Right to complain to the CIO if data is not processed in accordance with data protection principles.

6.3 Information Asset Owners should use guidance and templates made available by the Information Compliance Unit to create Privacy Notices unless otherwise justified by the circumstance.

7. Data sharing

7.1 All sharing of personal data with third parties will be subject to the appropriate controls as laid out in data protection legislation.

7.2 Repeated or ongoing data sharing arrangements must be covered by an appropriate data sharing or processor agreement.

8. Use of personal data within research

8.1 Where research involves the processing of personal data, the Chief or Principal Investigator will be considered to be the relevant Information Asset Owner for the data.

8.2 All requirements of this policy relating to processing of personal data should be adhered to alongside the company's research good practice requirements and code of conduct.

8.3 Use of personal data for research purposes will be subject to appropriate safeguards. In particular, personal data should be limited to the minimum amount of data which is reasonably required to achieve the desired research objectives. Wherever possible, personal information should be anonymised or pseudonymised so that the data subjects cannot be identified.

9. Governance Requirements

9.1 Implementation / Communication Plan

9.2 This policy is communicated to all staff as part of the company's induction process.

9.3 Exceptions to this Policy

9.4 There are no exceptions to this policy. Data Protection Legislation requires that all processing of personal data within the company be subject to an appropriate policy.

9.5 Review and Change Requests

9.6 This policy will be reviewed annually.

9.7 Legislative context

This policy is underpinned by the General Data Protection Regulations and the UK Data Protection Act 2018.

10. Change history

Policy version	Effective Date	Changes	Sign off
1.0	8th April 2019	Policy created	AMcG, LB
1.1	9th October 2020	Policy review. Updated with reference to SOP for Data Transfer and Processing and Reporting of Data Incidents	AMcG
1.2	11th November 2021	Policy review. Updated with reference to auditing, Information Asset Register and Record of Processing Activities location, document transfer via Slack.	AMcG, JCB
1.3	22nd December 2022	SOP review and update to branding / IG Officer	AMcG, JCB

Persons

AMcG: Andrew McGovern, Scientific Director

JCB: Joseph Babbage, Information Governance Officer