

Data Protection Policy

Oxford MeasurEd Limited

September 2023, updated March 2024



Contents

1. Purpose and scope	3
2. Principles of and protocols for data processing	4
3. Lawful basis for processing and consent	6
4. Data subject rights	6
5. Data breach notification	7
6. Third party processing	7
7. Privacy notices	7
8. Data protection impact assessments (DPIA)	7
9. Data Protection Officer (DPO)	8
10. Compliance and training	8
11. Policy review and updates	8
12. Further information and complaints	8

1. Purpose and scope

- 1.1 This Data Protection Policy outlines Oxford MeasurEd's commitment to safeguarding the privacy and security of personal and sensitive data. It serves as a guide for all employees, contractors, and partners (Oxford MeasurEd people) in handling data responsibly and in compliance with the United Kingdom General Data Protection Regulation law (UK GDPR).
- 1.2 In conjunction with Oxford MeasurEd's Risk Management Policy Framework, this policy aims to ensure comprehensive risk mitigation and compliance with data protection regulations.
- 1.3 This policy applies to all personal data processed by Oxford MeasurEd or any other individuals or organisations that handles data on behalf Oxford MeasurEd, including data collected from and about employees, clients, customers, research and evaluation participants. It also covers the storage, transmission, and deletion of personal data.
- 1.4 Michael Annoh, Director of Finance, is Oxford MeasurEd's Data Protection Officer (DPO) and responsible for the implementation of this policy.

1.5 Definitions

- 1.5.1 Personal data: Any information relating to an identified or identifiable individual.
- 1.5.2 Data subject: The individual to whom personal data relates.
- 1.5.3 Special category data: Personal data that needs more protection because it is sensitive. The UK GDPR defines special category data as:
 - (a) personal data revealing racial or ethnic origin;
 - (b) personal data revealing political opinions;
 - (c) personal data revealing religious or philosophical beliefs;
 - (d) personal data revealing trade union membership;
 - (e) genetic data;
 - (f) biometric data (where used for identification purposes);
 - (g) data concerning health;
 - (h) data concerning a person's sex life; and
 - (i) data concerning a person's sexual orientation.
- 1.5.4 Data processing: The collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, alignment, combination, erasure or destruction of data.
- 1.5.5 Controller: The entity that determines how and why personal data is processed.
- 1.5.6 Processor: The entity that processes personal data on behalf of the controller.

1.6 Who is this policy for?

- 1.6.1 Data protection is everyone's responsibility. This policy is to be implemented by all Oxford MeasurEd people.

- 1.6.2 All those working for and/or involved in research and evaluation with Oxford MeasurEd are to read the policy and have an opportunity to ask any questions where any aspects are not understood.
- 1.6.3 Oxford MeasurEd’s due diligence procedures include obtaining assurance that all sub-contracted organisations have sufficient policies and procedures in place to ensure that their work meets data protection standards in line with this policy.

2. Principles of and protocols for data processing

2.1 Oxford MeasurEd will adhere to the following data protection principles, as set out in the UK GDPR:

- 2.1.1 Lawfulness, fairness, and transparency: Personal data must be processed lawfully, fairly, and in a transparent manner.
- 2.1.2 Purpose limitation: Personal data will be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
- 2.1.3 Data minimization: Personal data collected must be adequate, relevant, and limited to what is necessary for the purposes stated.
- 2.1.4 Accuracy: Personal data must be accurate and, where necessary, kept up to date. Appropriate measures should be taken to rectify or erase inaccurate data.
- 2.1.5 Storage limitation: Personal data will be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed.
- 2.1.6 Integrity and confidentiality: Personal data will be processed securely, using appropriate technical and organizational measures to protect against unauthorized or unlawful processing and accidental loss, destruction, or damage.
- 2.1.7 Accountability: Oxford MeasurEd will be responsible for complying with the above principles and will be able to demonstrate compliance.

2.2 The table below sets out how Oxford MeasurEd will adhere to these principles.

Data protection principle	Adherence processes and protocols
Lawfulness, fairness, and transparency	<ul style="list-style-type: none"> • Oxford MeasurEd will ensure that there is a lawful basis for any processing of personal data (see point 3 below) • Oxford MeasurEd will produce and make available privacy notices for all activities that involve processing personal data that explain what personal data is being collected, who will have access to the data, how the data will be used, stored, processed and deleted, the legal basis for data processing, and how data subjects can raise a query or a complaint (see point 7 below).

<p>Purpose limitation</p>	<ul style="list-style-type: none"> • Oxford MeasurEd will only collect personal data for specific and legitimate purposes. These purposes will be explicitly recorded in a study plan and/or privacy notice (see point 7 below). • Oxford MeasurEd will not further process data in a manner incompatible with those specific purposes. • Oxford MeasurEd will never sell personal data and will only share personal data for specific and legitimate reasons (e.g. collaboration on a research or evaluation project). Data subjects will always be informed if information is going to be shared outside of Oxford MeasurEd.
<p>Data minimisation</p>	<ul style="list-style-type: none"> • Oxford MeasurEd will only collect personal data that is adequate, relevant, and necessary for the purposes of the processing. • For research and evaluation projects, this will be determined by the Project Director, including through the use of DPIAs for projects involving high risk or extensive processing (see point 8 below). • For company-level activities, this determined by Directors of Oxford MeasurEd.
<p>Accuracy</p>	<ul style="list-style-type: none"> • Personal data must be accurate and, where necessary, kept up to date. • Directors of Oxford MeasurEd will review company-level personal data (e.g. HR records) annually to ensure they are accurate and any inaccuracies are rectified. • For research and evaluation projects, appropriate measures will be taken to verify the accuracy of personal data.
<p>Storage limitation</p>	<ul style="list-style-type: none"> • For company-level activities, Directors will determine how long identification will be necessary (for example for the duration of a recruitment process, or a suitable time after reporting a safeguarding concern). This will be recorded in a privacy notice (see point 7 below). • The company may retain personal details of potential employees, collaborators or partners for longer than stated in a privacy notice at their request or with their written permission (for example for future recruitment opportunities). • For research and evaluation projects, the Project Director will determine how long personal data will need to be identifiable, including to allow for participants to withdraw their data from processing. This will be agreed with research funders/clients where appropriate and recorded in a privacy notice (see point 7 below). • If personal data is to be shared with any third-party processors, Oxford MeasurEd will ensure that appropriate data protection agreements are in place (see point 6 below). These will include deadlines for deletion of all personal data, which will be no later than the period necessary for the purposes of the third-party processing and any relevant quality assurance.

Integrity and confidentiality	<ul style="list-style-type: none">• All regular storage and processing of electronic personal data processed by Oxford MeasurEd is done using encrypted Microsoft cloud storage, with backup servers in UK or Ireland.• Oxford MeasurEd limits named access to electronic personal data to those authorised to have access and process the data for specified purposes.• Where electronic data is processed on other platforms or servers (e.g. survey platforms), the full details of this processing and storage and implications for data protection are provided in a privacy notice for data subjects.• Oxford MeasurEd limits hard copies of personal data. Where this is needed, protocols are agreed for securely storing, processing and deleting the copies.
Accountability	<ul style="list-style-type: none">• Oxford MeasurEd will conduct annual audits to ensure compliance with the above principles and procedures and the UK GDPR.• DPIAs for projects involving high risk or extensive processing will document all steps agreed to comply with the above principles and minimise risk (see point 8 below).

3. Lawful basis for processing and consent

- 3.1 Oxford MeasurEd will ensure that there is a lawful basis for any processing of personal data under Article 6(1)(a)-(f) of the UK GDPR. This includes consent from the individual for the performance of a contract, compliance with a legal obligation, protection of vital interests, consent, necessity for the performance of a task carried out in the public interest, or legitimate interests pursued by Oxford MeasurEd or a third party.
- 3.2 Where the lawful basis to process personal data is consent, Oxford MeasurEd will obtain explicit and informed consent from data subjects before processing their personal data, clearly explaining the purposes for processing and providing the right to withdraw consent at any time.

4. Data subject rights

- 4.1 Data subjects have the following rights regarding their personal data, in accordance with the UK GDPR:
- (a) Right to be informed
 - (b) Right of access
 - (c) Right to rectification
 - (d) Right to erasure (right to be forgotten)
 - (e) Right to restrict processing
 - (f) Right to data portability
 - (g) Right to object
 - (h) Rights related to automated decision making, including profiling

4.2 To enquire about exercising any of their rights as a data subject, individuals can contact Oxford MeasurEd's Data Protection Officer at michael.annoh@oxfordmeasured.co.uk.

4.3 If a child is under 13, an adult with parental responsibility holds these rights.

5. Data breach notification

5.1 In the event of a personal data breach, Oxford MeasurEd will adhere to UK GDPR requirements and promptly report the breach to the Information Commissioner's Office (ICO) if relevant.

5.2 Where the breach is likely to result in a high risk to the rights and freedoms of individuals, affected data subjects will be notified without undue delay.

6. Third party processing

6.1 If personal data is to be shared with any third-party processors, Oxford MeasurEd will ensure that appropriate data protection agreements are in place, outlining the responsibilities and obligations of each party in compliance with the UK GDPR.

7. Privacy notices

7.1 Under UK GDPR, there are certain things that we need to let data subjects know about how their information will be processed.

7.2. Oxford MeasurEd will produce and make available tailored privacy notices for activities that involve processing personal data (e.g. recruitment exercises, the company website, research and evaluation projects).

7.3 All privacy notices will explain what personal data is being collected, who will have access to the data, how the data will be used, stored, processed and deleted, the legal basis for data processing, and how data subjects can raise a query or a complaint.

7.4 Where relevant (e.g. international projects) privacy notices will explain any international transfers of data.

8. Data protection risk assessment

8.1 Safeguarding risks will be identified, assessed, monitored and evaluated at organisational- and project-level, as set out in Oxford MeasurEd's Risk Management Policy.

8.2 Where it is deemed appropriate (see below), Oxford MeasurEd will carry out Data Protection Impact Assessments to identify and mitigate risks on particular projects.

9. Data protection impact assessments (DPIA)

9.1 A DPIA is a process to help us identify and minimise the data protection risks of a project.

9.2 Oxford MeasurEd will complete a DPIA for any data processing that is likely to result in a high risk to individuals (as per the ICO screening checklist available at <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/accountability-and-governance/data-protection-impact-assessments/>).

- 9.3 Oxford MeasurEd may also choose to complete a DPIA for other data processing activities, for example projects where it is requested by the funder.
- 9.4 All DPIAs will be reviewed by Oxford MeasurEd's DPO.
- 9.5 All DPIAs must be approved by the Project Director or – in the case of company level activities – by a Director of Oxford MeasurEd.
- 9.6 Oxford MeasurEd's DPIA template ensures that a DPIA
- (a) describes the nature, scope, context and purposes of the processing;
 - (b) assesses necessity, proportionality and compliance measures;
 - (c) identifies and assesses the likelihood and severity of risks to individuals; and
 - (d) identifies any additional measures to mitigate those risks.
- 9.7 We will use Oxford MeasurEd's Risk Management Framework, as outlined in our Risk Management Policy, to undertake steps (c) and (d) above. If a DPIA identifies a high risk that cannot be mitigated, Oxford MeasurEd will consult the ICO before starting the processing.

10. Data Protection Officer (DPO)

- 10.1 Michael Annoh, Director of Finance, is Oxford MeasurEd's DPO.
- 10.2 The DPO is responsible for overseeing the implementation and enforcement of this policy, providing advice, and acting as a point of contact for data subjects and supervisory authorities.

11. Compliance and training

- 11.1 Oxford MeasurEd will conduct annual audits to ensure compliance with this policy and the UK GDPR.
- 11.2 Oxford MeasurEd will provide regular training to all employees in relation to data protection. All team members will complete the HSQE Data Protection and GDPR Awareness online training. This training will be refreshed every two years and more regularly if there are major changes to data protection legislation.
- 11.3 All Oxford MeasurEd employees and individual volunteers, contractors and consultants representing Oxford MeasurEd will be briefed on this policy.

12. Policy review and updates

- 12.1 This policy will be reviewed annually and updated as required to reflect changes in applicable data protection laws and regulations, as well as any changes in organisational practices.

13. Further information and complaints

- 13.1 If you have any questions with regards to how your data is handled by Oxford MeasurEd, please email the DPO at Michael.Annoh@oxfordmeasured.co.uk
- 13.2 If you would like to make a complaint to us about how your data is processed, please email Oxford MeasurEd's DPO at Michael.Annoh@oxfordmeasured.co.uk

- 13.3 If you are not satisfied with our response, or believe we are our processing of your personal data is not in accordance with the law, you can complain to the Information Commissioner's Office (ICO).