



CORONA
**MANAGEMENT
SYSTEMS**

INTERNAL POLICY DOCUMENT

DATA PROTECTION POLICY

Version 1.0 | Effective: October 2023

Table of Contents

1. Introduction.....	2
2. Scope	2
3. Definitions	2
4. Collection of Personal Data.....	2
5. Use of Personal Data	2
6. Storage of Personal Data.....	3
7. Disclosure of Personal Data	3
8. Data Protection Principles.....	3
9. Data Collection and Processing	3
10. Data Subject Rights - General Data Protection Regulation (GDPR) Rights	4
11. Data Breach Management.....	4
12. Data Sharing	4
13. Responsibilities.....	4
14. Training and Awareness	5
15. Policy Compliance	5
16. Complaints	5
17. Policy Review	5
18. CMS DATA PROTECTION STATEMENT	5
18.1 Collection and Use of Personal Data	5
18.2 What Personal Data We Collect	5
18.3 How We Use Your Personal Data	6
18.4 Legal Basis for Processing	6
18.5 Data Security and Confidentiality	6
18.6 Sharing of Personal Data	6
18.7 Data Retention.....	6
18.8 Rights of Data Subjects	7
18.9 Transparency and Accountability	7
8.10 Policy Updates.....	7
8.11 Contact Us	7
APPROVED BY:	8

1. Introduction

At Corona Management Systems (CMS) we are committed to protecting the privacy and confidential information of individuals and organisations we interact with. This Data Protection Policy sets out our procedures and guidelines for safeguarding personal data in compliance with applicable data protection laws and regulations including the General Data Protection Regulation (GDPR) Rights.

2. Scope

This Policy applies to all personal data collected by CMS . It applies to all employees, contractors, and third parties who process/handle personal data on behalf of CMS.

3. Definitions

Personal Data: Any information that can be used to identify an individual, directly or indirectly. It is any information relating to an identified or identifiable individual. This includes but is not limited to, names, addresses, email addresses, phone numbers, medical records, and financial information.

Data Subjects: Individuals whose personal data is obtained, stored, or processed by CMS.

4. Collection of Personal Data

CMS will only collect personal data that is necessary for a legitimate purpose and that is obtained with the consent of the individual. CMS will not collect personal data that is considered to be sensitive, such as racial or ethnic origin, political opinions, religious beliefs, or trade union membership, unless it is necessary for a legitimate purpose and the individual has explicitly consented to the collection of such data.

5. Use of Personal Data

CMS will only use personal data for the purposes for which it was collected and for which the individual has consented. CMS will not use personal data for any other purpose without the individual's consent.

6. Storage of Personal Data

6.1 CMS will take appropriate technical and organisational measures to protect personal data from unauthorised access, use, disclosure, alteration, or destruction. Personal data will be stored securely and will not be transferred without the individual's consent.

6.2 Appropriate security measures will be implemented to protect personal data from unauthorised access, disclosure, alteration, or destruction. These measures will be regularly reviewed and updated.

6.3 Risk assessments will be conducted to identify and address security vulnerabilities.

7. Disclosure of Personal Data

CMS will only disclose personal data to third parties with the individual's consent or where required to do so by law. CMS will take appropriate steps to ensure that any third parties to whom personal data is disclosed are also required to comply with this Policy.

8. Data Protection Principles

CMS is committed to upholding the following principles of data protection:

8.1 Lawfulness, Fairness, and Transparency: We will process personal data lawfully, fairly, and transparently. Data subjects will be informed of the purpose and legal basis of data processing.

8.2 Purpose Limitation: Personal data will only be collected for specific, explicit, and legitimate purposes and will not be further processed in a manner that is incompatible with these purposes.

8.3 Data Minimization: We will collect only the minimum amount of personal data necessary for the intended purpose.

8.4 Accuracy: We will ensure that personal data is accurate, and we will take reasonable steps to rectify or erase inaccurate data.

8.5 Storage Limitation: We will retain personal data for no longer than necessary for the purposes for which it was collected and in compliance with applicable laws.

8.6 Integrity and Confidentiality: We will implement appropriate technical and organisational measures to protect personal data against unauthorised access, disclosure, alteration, or destruction.

8.7 Accountability: We will be responsible for and demonstrate compliance with data protection principles.

9. Data Collection and Processing

9.1 Consent: Whenever possible, we will obtain explicit and informed consent from data subjects before collecting their personal data.

9.2 Legitimate Interests: In cases where consent is not appropriate, we may process personal data based on legitimate interests, but we will always balance these interests with the rights and freedoms of data subjects.

9.3 Data Subject Rights: We will respect and facilitate data subjects' rights, including the right to access, rectify, erase, or restrict processing of their data. They also have the right to object to the processing of their personal data and to data portability. Individuals can exercise these rights by contacting CMS Data Protection Officer.

10. Data Subject Rights - General Data Protection Regulation (GDPR) Rights

10.1 Right to Information: Data subjects have the right to be informed about the processing of their personal data.

10.2 Right of Access: Data subjects have the right to access their personal data.

10.3 Right to Rectification: Data subjects have the right to request the correction of inaccurate or incomplete personal data.

10.4 Right to Erasure: Data subjects have the right to request the erasure of their personal data under certain circumstances.

10.5 Right to Restriction of Processing: Data subjects have the right to request the restriction of processing their personal data under certain circumstances.

10.6 Right to Data Portability: Data subjects have the right to receive their personal data in a structured, commonly used, and machine-readable format.

10.7 Right to Object: Data subjects have the right to object to the processing of their personal data under certain circumstances, including direct marketing.

10.8 Automated Decision-Making and Profiling: Data subjects have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.

11. Data Breach Management

We have established procedures for identifying, reporting, and managing data breaches in compliance with applicable laws.

12. Data Sharing

We will only share personal data with third parties when necessary and with appropriate safeguards in place, including data processing agreements.

13. Responsibilities

13.1 Data Protection Officer (DPO): CMS will appoint a DPO to oversee and ensure compliance with this Data Protection Policy and relevant data protection laws.

13.2 Employees, Contractors, and Third Parties: All individuals who handle personal data on behalf of CMS must adhere to this policy and comply with data protection laws.

13.3 Data Breach Reporting: Any actual or suspected data breach must be immediately reported to the DPO, who will coordinate the necessary actions.

14. Training and Awareness

CMS will provide appropriate training and resources to all employees, contractors, and relevant third parties to ensure their understanding of data protection obligations and this policy.

15. Policy Compliance

Non-compliance with this policy may result in disciplinary actions, as well as legal consequences.

16. Complaints

Individuals who have any complaints about CMS handling of their personal data can contact the CMS Data Protection Officer or the relevant data protection authority.

17. Policy Review

This policy will be regularly reviewed and updated to ensure its ongoing effectiveness and compliance with evolving data protection laws and regulations.

18. CMS DATA PROTECTION STATEMENT

At Corona Management Systems(CMS), we are committed to protecting the privacy and personal data of individuals and organisations we interact with. This Data Protection Statement outlines how we collect, use, store, and protect personal data, in accordance with applicable data protection laws and regulations.

18.1 Collection and Use of Personal Data

We collect and process personal data for specific, lawful purposes, and only with the knowledge and consent of the individuals involved. The types of personal data we may collect include, but are not limited to, names, contact information, medical or health information, and research data. We use this data to fulfil our mission, provide services, conduct research, and comply with legal obligations. We will not use personal data for any purposes that are incompatible with those stated or required by law. CMS may anonymise your personal data and use it for research and statistical purposes

18.2 What Personal Data We Collect

- ✓ We may collect and process the following types of personal data:
- ✓ Name, contact details (e.g., email address, phone number)
- ✓ Identification information (e.g., date of birth, government-issued identification numbers)
- ✓ Health and medical information
- ✓ Research data and survey responses
- ✓ Other information you voluntarily provide to us

18.3 How We Use Your Personal Data

We may use your personal data for the following purposes:

- ✓ To provide you with our services, including research, public health programs, and related activities.
- ✓ To communicate with you, respond to your inquiries, and send you updates.
- ✓ To fulfil our legal and regulatory obligations.
- ✓ To conduct data analysis, research, and statistics (in a de-identified and aggregated format).

18.4 Legal Basis for Processing

We process your personal data based on one or more of the following legal bases:

- ✓ Your explicit consent.
- ✓ The necessity of processing for the performance of a contract with you.
- ✓ Compliance with legal obligations.
- ✓ Legitimate interests pursued by CMS.

18.5 Data Security and Confidentiality

CMS takes appropriate technical and organisational measures to safeguard personal data against unauthorised access, loss, or alteration. We restrict access to personal data to authorised personnel who have a legitimate need to access the information. We maintain confidentiality agreements with employees, contractors, and third parties who handle personal data on our behalf. We regularly review and update our security practices to ensure the ongoing protection of personal data. We are committed to protecting your personal data from unauthorised access, disclosure, alteration, or destruction. We implement appropriate technical and organisational measures to safeguard your information.

18.6 Sharing of Personal Data

CMS may share personal data with third parties, such as service providers and research partners, to fulfil our purposes and obligations. These may include:

- ✓ Authorised personnel within our organization.
- ✓ Trusted service providers, contractors, or research partners who assist us in our activities.
- ✓ Regulatory authorities when required by law.

We ensure that these third parties comply with applicable data protection laws and maintain appropriate security measures. We do not sell or trade personal data to third parties for marketing purposes without explicit consent.

18.7 Data Retention

CMS will retain personal data only for as long as necessary to fulfil the purposes for which it was collected or as required by applicable laws and regulations. When personal data is no longer needed, it will be securely deleted or anonymized, unless

retention is required by law or legitimate research purposes. We regularly review our data retention practices ensuring compliance with legal requirements and best practices.

18.8 Rights of Data Subjects

Individuals have certain rights regarding their personal data. These include the right to:

- ✓ Access your data and request a copy.
- ✓ Correct inaccuracies in your data.
- ✓ Portability
- ✓ Erase your data under certain circumstances.
- ✓ Restrict or object to the processing of your data.
- ✓ Not to be subject to automated decision making
- ✓ Withdraw your consent, where applicable.

We will facilitate the exercise of these rights, in accordance with applicable laws. Requests to exercise these rights can be made by contacting our Data Protection Officer (DPO) using the contact details provided in this statement.

18.9 Transparency and Accountability

We are committed to being transparent about our data protection practices. We have appointed a Data Protection Officer (DPO) who oversees our compliance with data protection laws and regulations. The DPO can be contacted with any questions or concerns regarding personal data or this Data Protection Statement.

8.10 Policy Updates

We may update this Data Protection Statement from time to time to reflect changes in our data protection practices or legal requirements. The most recent version will be available on our website.

8.11 Contact Us

If you have any questions, concerns, or requests related to your personal data or this Data Protection Statement, please contact us:

Corona Management Systems
Plot 2014 CAD Zone B09 Celina Ayom Street
Kado- Abuja
Nigeria

info@coronams.com

www.coronams.com

We are committed to protecting your privacy and ensuring that your personal data is treated with respect. If you have any questions about this Statement, please do not hesitate to contact us.

APPROVED BY:

NAME	POSITION	SIGNATURE	DATE
Tombari Duruzor	Director, People & Culture		
Chijioke Kaduru	Managing Director		

