CleanMax™
POWERING SUSTAINABILITY

Clean Max Enviro Energy Solutions Limited

DATA PRIVACY POLICY

June 2025

Document Control

A. Document Identification

Code	Name	Type
	Data Privacy	Policy

B. Roles and Responsibilities

Name	Title	Role[1]
Vishal Sangewar	Assistant General Manager	Author
Sweta Sajnani	Chief People & Culture Officer	Reviser
		Owner

C. Versions and History

Version	Date	Author(s)	Summary of Changes
1.0	14th June 2023	Vishal Sangewar	First Draft
1.1	17th June 2025	Sameer Patil	Updated role for cybersecurity specialist

D. Approval and sign off.

Name	Title	Status	Date
Deepak Singh	IT – DGM	Approved	20th June'25

E. Status and Classification

Version	Date	Status[2]	Classification[3]	Next Revision

1 Role: Author, Reviser, Advisor, Owner
2 Status: Draft, Approved, Published, Revised
3 Classification: IT Only, Internal Use, Public

Table of Contents

Purpose

The purpose of this policy is to ensure that Clean Max Enviro Energy Solutions Ltd. (CMES) and all its service providers involved in the processing of Personal Data is aware of, and complies with, applicable laws and regulations around data protection and privacy. This policy is applicable to CMES, and all the entities of CMES Renewable in India hereinafter collectively referred to as 'CMES'.

Scope

- This policy applies to all the employees, non-full-time employees and consultants and contractors etc. of CMES and all the renewable energy entity(s) in India in which CMES has direct or indirect investments and all their controlled subsidiaries (CMES).
- The tools and technologies mentioned in the policy will be deployed as per the Cybersecurity roadmap.

Audience

The target audience for this policy is CMES and all its service providers.

Roles & Responsibilities

Role	Responsibility
Assistant General Manager	• Implement, maintain, review, and update the Data Privacy Policy. • Communicate the Data Privacy Policy to intended audience. • Ensure all systems, services and equipment used for processing Personal Data meet acceptable security standards. • Perform regular checks to ensure that systems, services, and equipment used for processing Personal Data are functioning properly. • Evaluate the security posture of any third party CMES considers using to process Personal Data.
Cyber Security Specialist	• Implement, maintain, review, and update the Data Privacy Policy. • Ensure CMES carries out all activities related to Personal Data in compliance with applicable laws and regulations. • Act as the point of contact for all data protection and privacy matters. • Address inquiries and complaints of data subjects in a timely manner.

	• Review all processes and procedures around data protection and privacy and advise CMES regarding any updates that may be required. • Monitor effectiveness of implemented data protection and privacy controls. • Provide necessary consultation during a Data Protection Impact Assessment (DPIA). • Investigate potential Personal Data incidents with relevant functions/ teams to and track to closure. • Maintain an inventory of Personal Data incidents and record the lessons learnt.
Legal counsel	• Provide legal advice regarding applicable laws and regulations around data protection and privacy. • Conduct due diligence on any third party CMES is considering using to process Personal Data. • Manage all contracts/ agreements for CMES with its employees and associated third parties. • Provide necessary consultation during a Data Protection Impact Assessment (DPIA).
Assistant IT Manager	• Support the IT Head and the Cyber Security Specialist in their designated tasks.
Users	• Comply with the Data Privacy Policy in the fulfilment of their responsibilities.

Policy Statement

CMES requires processing of Personal Data for identified and documented business purposes. The security of such data is important for CMES as per industry standard and regulatory requirements. This policy outlines how the Personal Data shall be processed securely to meet the organization's data protection and privacy requirements. CMES shall ensure that all personnel who have access to any Personal Data are fully aware of and abide by this policy.

- The tools and technologies mentioned in the policy will be deployed as per the Information Security roadmap.

Definitions

Personal Data: Any information related to an identifiable person. Personal Data encompasses Personally Identifiable Information (PII) and Sensitive Personal Information (SPI).

Personally Identifiable Information (PII): Any information that permits the identity of an individual to whom the information applies to be distinguished or traced.

Sensitive Personal Information (SPI): Any information related to an individual which is private or could potentially harm the individual should it be made public.

Data Subject: An individual whose Personal Data is processed by CMES or by another entity on behalf of CMES.

Processing: Any operation or set of operations performed on Personal Data or on sets of Personal Data including but not limited to collection, storage, use, disclosure, transfer, or deletion.

Data Protection Principles

CMES shall discharge its responsibilities in accordance with the following adopted principles:

Lawful Basis of Processing

CMES shall process Personal Data of data subjects only on lawful grounds and after following the due process as laid down by applicable laws and regulations.

Privacy Notice

- CMES shall provide data subjects with the privacy notice as and when required.
- The contents and mode of presentation or delivery of the privacy notice shall be as per the requirements of the applicable laws and regulations.

Consent

- CMES shall obtain informed consent from data subjects prior to collection, use, or disclosure of Personal Data, wherever consent is relied upon as the legal basis for processing Personal Data.
- Data subjects shall, at any time during the lifecycle of their association with CMES or later, if applicable, have an option to withdraw any consent provided earlier.

Purpose Limitation

- CMES shall identify and document specific, explicit, and legitimate purposes for the collection of Personal Data.
- CMES shall collect and process Personal Data only for the identified purposes.

Data Minimization

- CMES shall collect Personal Data from data subjects limited to which is adequate and relevant to the identified purposes.
- CMES shall indicate clear distinction of the Personal Data being obligatory or optional for the identified purposes while collecting it from the user.

Data Retention and Disposal

- CMES shall retain Personal Data for only as long it is required for the fulfilment of the purposes of processing and/ or required by any applicable laws and regulations. CMES shall take reasonable steps to destroy or permanently de-identify and dispose Personal Data beyond this period.
- CMES may retain completely anonymized data for an extended time period if it is no longer capable of being used to identify any individual.

Accuracy

- CMES shall take reasonable steps to ensure that the Personal Data it collects, and processes is complete, accurate and up to date.
- CMES shall provide appropriate and adequate mechanisms to data subjects to communicate any changes or corrections to the Personal Data provided by them and have the same corrected or amended following due process.
- CMES shall further ensure that the requisite modifications are communicated to applicable third parties with whom the data has been shared.

Disclosure

- CMES shall ensure that a check is made to confirm that there are legal and/ or regulatory grounds for disclosing any Personal Data to a third party. Where such disclosure is required, the same shall be done after following due process laid down by the applicable laws and regulations in respective geographies.
- CMES shall ensure that only the minimum amount of Personal Data necessary is disclosed to third parties.

Transfer

- CMES shall transfer Personal Data to third parties or to external geographies, even within CMES, only if permitted by applicable laws and regulations.
- CMES shall transfer Personal Data with third parties only for reasons consistent with the purposes for which the data were originally collected or other purposes authorized by applicable laws and regulations.
- CMES shall transfer Personal Data to only those third parties who have similar levels of data protection and privacy controls as in CMES.
- Where Personal Data is being transferred across geographical boundaries, CMES shall comply with the requirements of applicable laws and regulations of the host and destination jurisdictions in relation to the transfer.

Security

- CMES shall implement appropriate technical and organizational safeguards to ensure the security of Personal Data, including the prevention of their alteration, loss, damage, unauthorized processing, or access, having regard to the state of the art, the nature of the data, and the risks to which they are exposed by virtue of human action or the physical or natural environment.

- CMES shall incorporate Privacy by Design wherever necessary in its processes and as required by applicable laws and regulations. It would be embedded at the initial planning/ design stages and throughout the complete development process of any new platform/ service/ product/ function/ process/ technology/ other activity that involves processing of personal data.

Accountability

CMES and applicable third parties shall be accountable towards data subjects for ensuring the protection and privacy of the Personal Data they process and shall demonstrate compliance with this policy.

Rights of Data Subjects

CMES shall provide data subjects with all applicable rights as mandated by applicable laws and regulations. CMES shall implement relevant mechanisms, processes, and procedures to facilitate these rights to data subjects.

Data Protection Governance

- CMES shall designate a qualified employee as Cyber Security Specialist to address data protection and privacy aspects arising out of applicable laws and regulations and be the point of contact for such matters.
- CMES shall equip the Cyber Security Specialist with the resources, support and training required to perform his/ her role.
- Name and contact details of the Cyber Security Specialist shall be communicated and accessible to all data subjects.
- The Cyber Security Specialist shall implement formalized processes to track and address any inquiries and complaints received from data subjects in a timely manner.
- CMES shall define roles and responsibilities at organization and function level to ensure the maintenance of data protection and privacy.
- CMES shall develop/ update processes and procedures around data protection and privacy from as advised by the Cyber Security Specialist.
- The Cyber Security Specialist shall monitor effectiveness of data protection and privacy controls on an ongoing basis and appropriate measures shall be taken by CMES to address identified deficiencies which shall be monitored for remediation.
- The Cyber Security Specialist shall report directly to the highest level of management on appropriate data protection and privacy compliance measures on a regular basis and shall additionally report as needed on ad-hoc high-risk matters.

Personal Data Classification

- CMES shall determine and document the criteria for Personal Data classification.
- Personal Data shall be classified into Personally Identifiable Information (PII) and Sensitive Personal Information (SPI). Further, required processes and controls as per the classification shall be implemented to ensure data protection and privacy accordingly.

Third Party Governance

CMES shall establish a third-party governance program to ensure.

- Appropriate due diligence covering data protection and privacy is carried out prior to onboarding any new third party.
- Contract signed with third parties cover requisite data protection and privacy clauses as well as clear instructions around how Personal Data shall be handled.
- Compliance of third parties to their data protection and privacy obligations is reviewed/ monitored at regular intervals of time.

Safeguards

Appropriate technical and organizational safeguards shall be implemented by CMES to ensure data protection and privacy, and shall include, but not be limited to, the following:

- Encrypt Personal Data when transmitting over public or untrusted network.
- Develop procedures for secure destruction or disposal of Personal Data and secure disposal of equipment or devices used for storing Personal Data.
- Develop a procedure for employees handling Personal Data outside organization premises through devices such as laptops, PDAs, etc. to securely execute activities without endangering the confidentiality and integrity of the data.
- Grant employees access only to the Personal Data necessary for the fulfilment of their duties.

Data Protection Impact Assessment

- CMES shall perform Data Protection Impact Assessment (DPIA) of the processing activities as and when required, as mandated by applicable laws and regulations.
- The Cyber Security Specialist and Legal Counsel (where necessary) shall be consulted while carrying out the DPIA.
- For any high risks identified during DPIA, where appropriate mitigation measures do not exist, the Cyber Security Specialist shall consult with the relevant data protection authorities prior to starting the processing.

Record Management

- CMES shall keep records of all processing activities involving Personal Data in formats mandated by applicable laws and regulations.
- CMES shall secure and preserve access to records and destroy them as soon as they are no longer required.
- CMES shall have mechanisms in place to track offsite storage of paper records and transfer of electronic documents.
- Upon request, CMES shall disclose records to data protection authorities, auditors and any other entity as required by applicable laws and regulations.

Compliance

- CMES shall have its data protection program audited by an internal audit team annually or as may be required by applicable laws and regulations.
- CMES shall develop key performance indicators (KPIs) for measuring the compliance and performance of the current processes related to data protection and privacy.
- The Cyber Security Specialist shall track and monitor the KPIs on a regular basis and identify appropriate remedial actions if required.

Non-Disclosure and Confidentiality Agreements

- CMES shall incorporate requisite non-disclosure and confidentiality clauses in its agreements and/ or contracts with employees as well as individuals external to the organization who are privy to the Personal Data being processed by CMES or its associated third parties.
- CMES shall ensure that its employees and associated third parties sign the non-disclosure and confidentiality agreements covering data protection and privacy responsibilities on or before their joining date.
- CMES employees and associated third parties involved in any stage of processing Personal Data shall explicitly be made subject to a requirement of secrecy which shall continue after the end of the employment relationship.

Personal Data Incident Management

- CMES shall establish necessary processes and controls to manage information security incidents (also referred to as breaches) related to Personal Data.
- The Cyber Security Specialist shall work closely with relevant functions/ teams to investigate potential Personal Data incidents and track to closure.
- The Cyber Security Specialist shall maintain an inventory of such incidents and shall record the lessons learnt.
- In the event of a Personal Data incident, CMES shall follow the processes laid down by applicable laws and regulations regarding notification of the breach. Notification may be to the applicable regulatory authority, the data subjects impacted, and any other entity as prescribed by the applicable laws and regulations.
- The notification of any personal data breach should include the areas which have been identified as part of the Appendix A of this document.
- However, in addition to Appendix A it is necessary to identify additional requirements which may be necessitated as per the applicable laws and regulations.
- CMES shall ensure that its employees and associated third parties are aware of the mechanism of reporting information security incidents, including Personal Data incidents.

Exceptions

Where there is a justifiable business need that requires actions to be performed which are in conflict to this document, such exceptions shall be reported to the management team along with risk and approval

obtained. Such approvals shall be valid for a pre-defined period mentioned in exception form/ request, after which it shall be re-evaluated and re-approved.

Glossary

CMES	Clean Max Enviro Energy Solutions Ltd.
DPIA	Data Protection Impact Assessment
PII	Personally Identifiable Information
SPI	Sensitive Personal Information

Appendix A

Area	Description
Nature of the Breach	How the breach happened, how many individuals were affected, categories of data affected, how many records were lost, exposed, etc.
Contact Persons	Name and contact details of the entity considered the point of contact for data protection within the organization should be mentioned.
Consequences of the Breach	The results of the breach need to be explained wherein consequences such as identity theft, financial damages, etc. should be identified due to the loss or exposure of data.
Measures Taken	Details of the remediation to address the breach should be mentioned. This should include how to solve the immediate problem – for example how to decrypt or restore the data – and how to prevent and mitigate similar incidents in future.