Data Privacy & Protection Policy

Version 2.0

Approval and Effectiveness

This Policy was initially issued on 2nd May 2025. The Policy was subsequently reviewed and revised (Version 2.0) and approved by the Board of Directors of Saatvik Green Energy Limited in its meeting held on 11th December 2025. The revised Policy is effective from the same date and shall remain in force until amended or replaced by the Board/ESG Council of Saatvik.

1. Introduction

Saatvik has established a Data Privacy & Protection Policy which supports the strategic aims of the business and is committed for maintaining and improving data security posture within the organisation and minimizing its exposure to all risks.

When used properly, Information (data) helps companies to better understand the needs and desires of their interested parties. It also forms the basis to automate the process that help companies to evolve their operations. With the increasing use of digital platforms, issues like data protection and privacy have become more prominent in the public eye. At Saatvik Group ("Saatvik", "We", "Our"), we understand the concerns that can arise due to mishandling of collected information that is personal in nature and are committed to applying the highest standards of fairness, transparency, and accountability in managing personal data.

Saatvik is committed to safeguarding the privacy and confidentiality of any information entrusted to its care. Saatvik is dedicated to upholding this fundamental responsibility by ensuring the proper safeguarding and utilization of personal information, also known as "Personal Data", gathered by us.

2. Purpose

This policy's objective is to protect the personal information of current, former, and potential workers, clients, and associates in relation to the gathering, use, and sharing of personal data.

3. Scope

This policy is applicable to all personal data collected, stored, or processed across operations of Saatvik Green Energy Limited and its subsidiaries (collectively referred to as the "Saatvik Group" or "Saatvik"), covering employees, job applicants, contractors, consultants, vendors, suppliers, customers, digital users, and any third parties whose data we process. The policy is applicable:

- irrespective of the form of its presentation or the medium used (paper, tape, film, electronic media etc.)
- irrespective of whose order, on whose behalf, or for whose account such information is stored,
- regardless of how such knowledge is acquired (directly, through seeing, hearing, etc., or indirectly, through accessing a document that contains information, etc.).
- regardless of any other characteristic of such information, hereinafter referred to as personal data.

4. Definitions

S. No.	Term	Definition
1.	**Applicable Laws**	**"Applicable Laws"** shall mean and include all applicable laws (including the DPDP Act, the IT Act, the IT Rules and the Consumer Protection (E-Commerce) Rules, 2020 and such other similar laws / legislations which may be enacted from time to time), statutes, legislative enactments, ordinances, judgments, decrees, declarations, notifications, guidelines, circulars, directives, codes, injunctions, writs, rules, bye-laws, regulations, policies, directions, demands, assessments, conventions, orders, interpretations, licenses, permits, authorisations, standards and requirements of all government authorities, and all government approvals, whether in effect on the date of this Privacy Policy or thereafter.
2.	**IT Act**	"**IT Act**" shall mean the Information Technology Act, 2000, of India and the rules prescribed thereunder, as amended, substituted, modified or re-enacted from time to time.
3.	**IT Rules**	"**IT Rules**" shall mean the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, as amended, substituted, modified or re-enacted from time to time.
4.	**Data**	"**Data**" means a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means.
5.	**Personal Data**	❖ Data which relates to an individual who can be identified from that data; or ❖ Expression of opinion about an individual ❖ Personal data may include any personal details such as name, address, telephone numbers, email IDs, work experience information, health records, PAN number, driving license number, etc.

S. No.	Term	Definition
6.	**Sensitive Personal Data**	❖ Any personal data that contains an opinion about a person or may induce the formation of an opinion that may negatively impact an individual personally or professionally. ❖ Any personal data from which an implication of criminal conduct can be drawn. ❖ Sensitive personal data includes all kinds of national ID numbers, financial data, religious beliefs, political opinions, physical or mental health conditions, sexual life, or any criminal proceedings / dispositions relating to an individual. For the purpose of compliance, only what is specified in the IT Act 2008 needs to be included (SPI and PII).
7.	**Critical Data**	Data whose compromise could severely impact operations, reputation, legal compliance, or customer trust.
8.	**Data Subject**	The living individual who is the topic / subject of the personal data.
9.	**Data Fiduciary**	"**Data Fiduciary**" means any person who alone or in conjunction with other persons determines the purpose and means of processing of Personal Data.
10.	**Data Principal**	❖ **"Data Principal"** means the individual to whom the Personal Data or Information relates and where such individual is— • a child (who has not completed the age of 18 years), including the parents or lawful guardian of such a child; • a person with disability, including her lawful guardian, acting on her behalf.
11.	**Data Controller**	The entity / organisation that determines the purposes and means of processing personal data (i.e., the client).
12.	**Data Processing**	This includes seeing, accessing, gathering, recording, organising, storing, changing, using, disclosing, deleting, and transferring personal data, as well as any other action involving personal data.
13.	**Data Processor**	The entity / organisation that processes personal data on behalf of a data controller, as per their direction and instruction (i.e., GKB, as a service provider).
14.	**Data Transfer**	This is the transfer of personal data from one location to another; it includes viewing or accessing personal data held locally from an offshore location.

S. No.	Term	Definition
15.	**DPDP Act**	"**DPDP Act**" shall mean the Digital Personal Data Protection Act, 2023, of India and the rules prescribed thereunder, if any, as amended, substituted, modified or re-enacted from time to time.
16.	**Pseudonymisation**	When the real data can be isolated from other stakeholders by giving it a pseudonym (for instance, employee ID rather than employee name), pseudonymisation should be used so that processing can proceed using the pseudonym.
17.	**Anonymisation**	It is no longer possible to identify the data subject. When it is necessary to completely conceal or anonymise the actual data, employ anonymisation. For instance, data stored in the DEV database can be anonymised since the developers have no legitimate reason to view the actual data on the DEV server.

5. Roles & Responsibilities

S. No.	Roles	Responsibilities
1.	**Information Security Steering Committee**	❖ Review & approve policies ❖ Provide strategic oversight and risk governance towards the implementation of the policy ❖ Ensure resource allocation and compliance posture
2.	**Data Protection Officer (DPO) / CPO**	❖ Advise on privacy-related policy ❖ Oversee personal and sensitive data handling ❖ Respond to regulatory and data subject requests
3.	**Chief Information Security Officer (CISO)**	❖ Define and enforce security controls per classification level ❖ Conduct risk assessments and incident response ❖ Support the implementation of ISMS and other relevant information security frameworks
4.	**Board of Directors**	❖ The Board of Directors and Managing Director hold ultimate accountability for data privacy compliance and oversight. They delegate operational responsibilities to the DPO, CISO, and relevant committees.

5. Applicability

This policy is applicable to all employees, partners, consultants, contractors, third-party vendors, interns, and outside organisations who use, oversee, or are given any organisational property that SGEL owns, leases, or otherwise manages.

6. Enforcement

Violations of this policy may attract disciplinary action, based on the specifics of the infraction, which could lead to Termination of employment or contract. Moreover, depending on the type of infringement and the area, civil, criminal, and/or other relevant legal actions may ensue.

7. Access, Collection, Processing, Use and Disclosure of Personal Data

7.1 Saatvik obtaining information of the Data Principal from publicly and commercially available sources and from our platform and associated applications, accessible through any internet-connected devices, will not capture any Personal Data or Information of the Data Principal without the explicit consent of the Data Principal. Currently, there is no requirement for the Data Principal to submit Personal Data for browsing, accessing, or using our services. However, we may collect and process Personal Data voluntarily provided by the Data Principal, with their consent.

7.2 Saatvik will collect/use/process the Personal Data or Information in accordance with what has been stated in the DPDP Act and IT Rules (including any amendments thereto) and any other Applicable Laws for the time being in force.

7.3 Throughout the course of the relationship or interaction with the Data Principal, Saatvik, collecting the Personal Data will use solely for the intended purposes, and such Information of the Data Principal shall be shared only with authorized personnel to facilitate service access and shall ensure data security.

7.4 In case of any inaccurate/incorrect information provided by the Data Principal can be rectified by the Data Principal by placing a written request addressed to the Grievance Officer for correction, completion, updating or erasure of the Data Principal's Personal Data or Information for the processing of which, the Data Principal had previously given consent

7.5 Data Principal has the right to withdraw consent for data processing by contacting the Grievance Redressal Officer. Such requests will be thoroughly verified before processing. Withdrawal of consent may limit access to our services, but it does not affect the legality of the processing of Personal Data or Information for which the consent was provided before its withdrawal.

7.6 The Data Fiduciary only collects, uses and discloses Personal Data for purposes that are reasonable and legitimate. Such Personal Data shall be processed in a manner compatible

with the agreed purposes; unless the Data Principal has consented to it being processed for a different purpose or a different purpose is permitted by applicable law.

7.7 The Company may, from time to time, disclose and/or transfer the data subject's Personal Data to third parties (including but not limited) those listed below:

- Group companies, affiliate companies and/or other business associates, the Company's insurers and banks;
- External and internal auditors;
- Administrator of the Company's mandatory provident fund scheme;
- Third parties who are involved in a merger, acquisition or due diligence exercise associated with the Company.
- External companies or third parties that the Company engages to perform services on the Company's behalf;
- Third Parties providing certain information technology and data processing services to enable business operations;
- The applicable regulators, governmental bodies, tax authorities or other industry recognised bodies as required by any Applicable Law or guidelines of any applicable jurisdiction; and
- To any other party as deemed necessary by the Company.

7.8 Notwithstanding anything contained elsewhere, any Personal Data may be disclosed by the Company to any third party as required by a Court of Law or any other regulatory or law enforcement agency established under a statute, as per the prevailing law, without the data subject's consent.

7.9 The Company shall present a request for consent with an option to access such request in English or any other language, in compliance with Applicable Laws. Such request shall be accompanied or preceded by a notice given by the Company to the Data Principal ("Notice") inter alia informing the Data Principal about the Personal Data or Information that may be Processed, the purpose for which it is proposed to be Processed, Data Principal rights under Section 6(4) (Right to withdraw consent for the processing of Personal Data) and Section 13 (Right to Grievance Redressal) of the DPDP Act and the manner in which the Data Principal may make a complaint under the provisions of the DPDP Act.

7.10 Transmission of Personal Data

- On occasion, we may disclose Personal Data and it may be accessible to authorized Internal recipients within Saatvik, its subsidiaries or our authorized service providers including cloud service providers who provide services to Saatvik, tax consultants and authorities, Government Bodies including statutory, regulatory authorities, law-

enforcement agencies (where applicable), Auditors (internal/external), depositories, Registrar & Transfer Agents.

- Consequently, on occasion, Customers, Vendors, Suppliers' Information might be transferred to said other organization and the concerned Information will always be safeguarded by the organization, irrespective of its location of use or transfer.
- In addition, the organization may divulge affiliate information in situations where such disclosure is required to adhere to a legal or statutory duty.

8. Data processing for the provision of the website and creation of log files

By default, when the Data Principal visits our website, our web servers obtain and collect the name of the Data Principal's internet service provider, the Data Principal's IP address, the website from which the Data Principal is visiting us, and the date and duration of the visit. This data is stored in the log files of our systems and is used for problem or error analysis. However, the use of the IP address is limited to the technically necessary extent and is abbreviated and therefore used only anonymously, so that it is not possible to assign the IP address to a Data Principal. The data is not merged with Personal Data.

The temporary storage of the abbreviated IP address by our systems is technically necessary to display the website to your terminal device. Storage in log files is done to ensure the functionality of the website.

The collection of data for the provision of the website and the storage of data in log files is essential for the operation of the website. Therefore, there is no possibility for the Data Principal as a user to object to such processing.

9. Data processing in respect of services offered on the website

On our website various services are offered, for the use of which we request Personal Data from the Data Principal.

9.1 Data processing in the context of marketing activities (DOI, Tracking)

We want to provide the Data Principal with information that is individually tailored to the Data Principal's interests as much as possible. In order for the Data Principal to use these services, we will require Personal Data from the Data Principal, such as the Data Principal's name, e-mail address, company and/or telephone number, which the Data Principal can provide to us via a registration form on one of our registration pages, as well as the Data Principal's combined consent.

- In the sending of personalized advertising and information, for e.g., newsletters, invitations, trade fairs and events, products, services, offers and promotions, including

opinion surveys and company communications by e-mail, SMS and/or instant messenger services.

- In the tracking of Data Principal user behavior in connection with digital Saatvik offers, which sections, articles, products, and other content on our websites, and which links in our e-mails on our websites did you use and when; how did you interact with our services, e.g, participation in a webinar.

The data will be deleted as soon as they are no longer required to achieve the purpose for which they were collected. Therefore, the data is stored as long as the registration for the personalized advertising and information service is active. At any time, the Data Principal can revoke the Data Principal's consent to the processing of Personal Data by e-mail to dpo.support@saatvikgroup.com or by clicking on the "unsubscribe link" in the received messages, with effect for the future and thereby unsubscribe from the service. In this case, all Personal Data stored in the course of contacting us, as well as Information about the Data Principal's usage behavior, will be deleted. The revocation of consent does not affect the lawfulness of the processing carried out on the basis of the consent until the revocation.

9.2 Use of Saatvik Contact and Get in Touch Form

- The website has a contact and get in touch form that can be used to contact us electronically.
- To use the get in touch form, the Data Principal must fill the mandatory information in the respective input mask marked by an asterisk (e.g., your e-mail address). All other information is optional for the Data Principal. This Personal Data will be sent to a department of ours that is responsible for processing and storing it in our systems. At the time of sending the message, the date and time of the entry will be saved. We will obtain the Data Principal's consent for processing of the data during the inquiry process.
- The data filled in the input mask will be used exclusively to process your inquiry.
- The Data Principal has the right to withdraw their consent to the processing of Personal Data at any time by sending an e-mail to dpo.support@saatvikgroup.com. In this case, all Personal Data stored as part of the contact will be deleted with effect from the date of withdrawal. Data Principal's request would be honoured and answered within 15 working days from the date of raising the request.
- Contacting is also possible via WhatsApp through the link/number provided by us on the website. The previous statements on data processing apply accordingly. If the Data Principal uses them, the processing of the Data Principal's Personal Data is based on our legitimate interest.

9.3 Data processing in connection with Cookies, Web Beacons and Local Storage

i. **Cookies**:

We use cookies to enable the Data Principal to make the best possible use of the website. Cookies are text files that are stored in the internet browser or saved by the internet browser on the terminal device of the Data Principal. If the Data Principal visits our website, a cookie can be stored on the Data Principal's operating system. This cookie contains a characteristic string that allows clear identification of the browser when the website is accessed again. We also use cross-domain cookies, which are used to transfer session information from one or more other domains. This means that Data Principal data can be used not only on the generating domain but also on other Saatvik's websites. The requirement for the use of cross-domain cookies is that they are used on websites within an application, and identical cookies are used on the websites and make our websites more user-friendly.

In the following, we provide you with general information about the use of cookies on our website and the associated processing of personal data. For further information on specifically used cookies, please refer to the Saatvik Cookie Policy published on this website.

We use cookies to make our website more user-friendly. Some elements of our website require the requesting browser to be identified even after a page break.

In addition, we use cookies on our website to allow the analysis of the Data Principal's surfing behavior.

When visiting our website, the Data Principal is informed about the use of cookies and referred to this Policy.

Some features of our website cannot be offered without the use of cookies. It is necessary that the browser is recognized even after a page break. The Data Principal's data collected through the technically necessary cookies will not be used to create user profiles. Further information can be found in the Saatvik Cookie Policy.

Analysis cookies are used to improve the quality of our website and its content. Analysis cookies show us how the website is used.

Cookies are stored on the Data Principal's terminal device and transmitted from it to our website. Therefore, the Data Principal as a user also has full control over the use of cookies.

By changing the settings in your internet browser, Data Principal can disable or restrict the transmission of cookies. Cookies that have already been stored can be deleted at any time. This can also be done automatically. If cookies are deactivated for our website, it may no longer be possible to use all functions of the website in full.

ii. Web –Beacons

Web beacons are small graphic files (also referred to as "counting pixels", "pixel tags" or "clear GIFs") that may be included in our websites, apps, applications and newsletters and are usually used in conjunction with cookies. The above statements on cookies apply accordingly to web beacons; web beacons are not used in particular if the Data Principal has objected to the use of the relevant cookie.

Web beacons serve statistical purposes and purposes of personalization in the further development and relevance of the website and represent a legitimate interest of Saatvik.

iii. Local Storage

We use the functionality of the so-called local storage. The Data Principal's data (master data, status data and program data) are stored locally in the cache of their browser. If the Data Principal doesn't delete the cache of their browser, this information is retained and can be read out the next time the Data Principal visits the website. By using local storage, we enable the Data Principal to view their data correctly while browsing on our website without slowing down this process unnecessarily and overloading the interfaces.

If the Data Principal does not wish to use the local storage, the Data Principal can set this accordingly in the settings of their respective browser at any time. Please note that, in this case, the functionalities of our website will only be available to the Data Principal to a limited extent or will no longer be available.

9.4 Data Processing in connection with social media networks

The following information of the Policy applies to the Saatvik Group's appearances on social media or third-party platforms:

LinkedIn

Instagram

YouTube

Facebook

The declaration below on the processing of Personal Data refers purely to the processing by the Saatvik Group itself. The providers of the listed social media processes Personal Data of registered users, but also of non-registered visitors to their websites by applying their own policies. They are responsible for their own user data processing policies. The user or visitor should be informed about the data processing by the social media sites directly from the social media providers.

The respective legal entity within the Saatvik Group's legal entities is responsible for the collection of data for the above-mentioned social media presence.

We collect and process Personal Data in the course of the use of our social media sites by the Data Principal and may transfer Information to an internal system for Processing regarding this purpose.

i. Processing of Data Principal Personal Data when contacting us

If Data Principal provides us with Personal Data by contacting us, e.g., by e-mail or by a direct message within social media, WhatsApp message or text message, we process the Data Principal's Personal Data for the purpose of fulfilling the contract or for the implementation of pre-contractual measures that are carried out in response to the Data Principal's request due to our legitimate interest in answering the Data Principal's request. Thereby, we process the Personal Data that the Data Principal provides to us directly via inquiry. It may also happen that we visit the Data Principal's public profile and store data from it, provided that this is necessary for the above-mentioned purposes.

The processing of the Personal Data is carried out on the basis of Saatvik's legitimate interest in providing the Data Principal with targeted information about us and our services, as well as the optimized design of our social media presences and effective communication with the Data Principal.

ii. Processing of Saatvik's Personal Data within social media networks

For all our social media presences, we receive messages about whether users of the social media give a "like" for our posts, finds them interesting, shares or recommends or comments (depending on the function of the social media), etc. We may also see a list of our respective followers or subscribers, and on some social media sites (for example, XING), a list of visitors to our social media presence. In addition, we can see when the Data Principal leaves reviews about our company, provided that this review is linked to the respective social media platform.

iii. Processing of statistical data within social media networks

We also receive statistical evaluations of the use of our social media sites from all social media providers. Beyond the information mentioned under 6.3.1, however, this only contains anonymized information, such as (depending on the provider) demographic data, an anonymized analysis of the interaction and reach of our social media presences and posts, and anonymized information such as languages, interests and end devices used by our users.

iv. Processing of Data for advertising purposes and creation of usage profiles by the providers of the social media networks

The data mentioned under 10.4.1 and 10.4.2 may also be processed for market research and advertising purposes. This happens, for example, when we place advertisements on the respective social media. However, the data is processed by the respective providers. Please also note that they can create usage profiles from your usage behaviour. These usage profiles can, in turn, be used, for example, to place advertisements within and outside the platforms that correspond to your developed interest profile. Please inform yourself about this with the providers of the social media.

10. Purpose of collecting personal data

The subsequent categories of Personal Data may be acquired by us via direct interactions with individuals, information obtained from client engagements, applicants, suppliers, and other circumstances.

The Data Fiduciary may collect, process and disclose Personal Data of the Data Principal for purposes connected with its business activities, including the following purposes:

10.1 Personal Details, such as your name, gender, nationality, employee photos, date of birth, driver's license, languages spoken, and other personal details which can be used to identify you;

10.2 Contact details, such as private addresses, phone numbers, email addresses, emergency contacts such as next of kin, and other contact details;

10.3 Financial information, such as banking details, tax information and other financial information;

10.4 IT and facility information, such as information required to provide access to our IT-systems and networks, such as IP addresses, device addresses, use of our resources and facilities, log files, login information, sites visited, software and hardware inventory, IT incidents and history, and e-mails sent and received using our platforms;

10.5 Other personal data you choose to share with us;

Sensitive Personal Data: Apart from our own Employees, we do not generally gather sensitive or special categories of Personal Data. Saatvik may be required to process the Sensitive Personal Data of our Employees and would only process such data when required to do so for the purpose of protecting the interest of individuals, establishing, or defending legal claims, exercising its rights and obligations as an employer (including for occupational health purposes), or with the explicit consent of the individual or individuals involved.

The following are instances of Sensitive Personal Information that we might acquire or retain:

a) Personal identification documents that have the potential to disclose information such as –
   - Unique identification numbers, such as driving license numbers, passport numbers and other government-issued ID numbers.
   - Biometric data, such as fingerprints and retinal scans.
   - Financial information, including bank account numbers, PAN Number, etc.
   - Medical records.
   - Religion
   - Gender

b) Data furnished by our consumers during the progression of our professional collaboration.

c) Applicants voluntarily disclose diversity and equal opportunity information during the recruitment process.

d) To ensure a secure environment for our Employees, Health Data may be processed as required

11. Policy Compliance

11.1 This Policy is applicable to all existing employees, prospective employees, and persons (Users/Data Principal) who visit the office/branch and/or any digital data of the Company and its subsidiaries.

11.2 Company IT / HR / Internal Audit team will verify compliance with this Policy through various methods, including but not limited to, virtual monitoring, business tool reports, internal and external audits, and feedback from data subjects.

11.3 Saatvik will conduct regular training and awareness programs for employees, contractors, and third parties on data privacy, responsible data use, cyber hygiene, and breach reporting. Specialised training will be provided to HR, IT, and managers handling personal data.

12. Data Processing Contracts

12.1 The Company may engage, appoint, use or otherwise involve a Data Processor to process Personal Data or Information on its behalf for any activity related to offering of goods or services to Users under a valid contract.

12.2 The Company shall ensure that its Data Processors take reasonable security safeguards to prevent any unauthorised Processing of Personal Data or Information or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to Personal Data or Information that compromises the confidentiality, integrity or availability of Personal Data or Information.

13. Information Security and Confidentiality

13.1 The Company implements comprehensive technical, organizational, and physical safeguards to protect Personal Data from unauthorized access, alteration, loss, or destruction. Our security protocols are regularly updated to comply with legal standards and include measures such as encryption and physical security to prevent unauthorized system access. Despite rigorous security practices, the absolute security of data transmitted over the internet or stored in our systems cannot be guaranteed. Publicly shared information on discussion forums is accessible to anyone online.

13.2 Personal Data, including any sensitive financial information collected, if any, on devices or computers or servers that may be protected by physical, as well as reasonable technological security measures and procedures, in accordance with the IT Act and the IT Rules and any other Applicable Laws.

13.3 The Company affirms that it does not sell or share such Personal Data with third parties, except as required by law, and takes utmost faithful measures to provide security measures that are integrated at various levels, including data masking, user access restrictions based on roles, and infrastructure and intellectual property protection through firewalls.

14.1 Any complaints, abuse or concerns with regard to content and /or comments or any breaches of these terms shall be immediately notified to the designated Grievance Officer as mentioned above.

14. Data Retention

14.2 Adhering to the DPDP Act, we are committed to ensuring the confidentiality and protection of the Data Principal/user's Personal Data and Information, and for this purpose, Saatvik will retain the Data Principal/user's Personal Data and Information only for the duration necessary to fulfil the purposes for which it was collected, in strict compliance with applicable legal requirements. This entails that the Personal Data and information will be

kept for the period during which the Data Principal/user engages with our services and for any additional time that may be mandated to ensure adherence to legal obligations.

14.3 Upon the cessation of Data Principal/user's use of our services in the Saatvik or when it is determined that the Personal Data and Information is no longer required for the originally specified purposes or to satisfy any legal, regulatory, or statutory obligations then Saatvik will proceed to either erase, delete, or anonymize Data Principal/user's Personal Data and Information within a timeframe that is considered reasonable.

14.4 This action is taken unless there is a legal basis that necessitates the continued retention of such Data, including but not limited to compliance with specific laws that dictate longer retention periods, or the need to retain the Information for the purposes of addressing legal claims or disputes.

15. Right To Erasure

15.1 The Personal Data has to be erased for compliance with a legal obligation, and to comply, the Data Principals can request erasure of their personal data under the following conditions:

- The Personal Data is no longer necessary in relation to the purposes for which it was collected or otherwise processed.
- The Data Principal withdraws consent on which the Processing is based, and where there is no other legal ground for the processing.
- The Data Principal objects to the Processing, and there are no overriding legitimate grounds for the processing.
- The personal data has been unlawfully processed.

15.2 The Data Principals who are exercising their right to erasure should submit a formal request to the Data Fiduciary of the Company via (contact email) or (contact address). The request should specify the data or categories of data to be erased and the reason for the erasure request.

15.3 The Company will evaluate each request in accordance with the Act and inform the Data Principal of the decision within 90 days of receiving the request. If the Company decides to erase the requested data, it will take reasonable steps to inform other entities that are processing the said data about the erasure request.

16. Grievance Redressal

16.1 All Data Principal may address any questions, discrepancies, or grievances regarding the processing of Personal Data to the legal team of Saatvik Group.

16.2 The role of the Grievance Officer is to:

- Redress Data Principal grievances expeditiously;

- act as a point of contact between Data Principal and Saatvik;
- respond to any communication from Data Principal for the purpose of exercising of Data Principal's rights under the DPDP Act, IT Act and IT Rules.

16.3 The Grievance Redressal Officer shall endeavour to acknowledge the Data Principal's complaints within 2 working days of the receipt of such complaint, and shall seek to address and/or resolve the same within a period of 15 working days of the receipt of such complaint. The Data Principal further understands and agrees that the decision of the Grievance Redressal Officer shall be final and binding in this regard.

17. Changes in the Privacy Policy

The Company solely reserves the right to revise and/or modify and/or amend and/or substitute this Policy at any time, without any prior notification to Data Principal. If we decide to change our Policy, we will post those changes to this Policy in an appropriate place, along with a change notice where we feel that it is necessary and/or possible to do so. All such revisions, modifications, amendments, and substitutions shall be effective immediately upon posting of the same by Saatvik, and you, the Data Principal, will be deemed to have absolutely, unconditionally and irrevocably accepted all such revisions, modifications, amendments and/or substitutions. By assenting to the terms of this Policy, Data Principal agrees to periodically review this Policy, acknowledge to have read and understood any and all revisions, modifications, amendments and/or substitutions to this Policy and Data Principal further confirms to unconditionally bound by any and all such revisions, modifications, amendments and substitutions thereto by Data Principal's continued access or use of the services.

18. Dispute Resolution and Governing Laws

18.1 This Privacy Policy shall be governed by, and construed in accordance with the laws of India, without regard to the conflicts of law rules thereof.

18.2 Any and all disputes arising out of or in connection with this Policy will be subject to the jurisdiction of the Courts of Gurugram.

18.3 Data Principal expressly acknowledges and agrees that Saatvik shall not be obliged or responsible for complying with the laws of any jurisdictions (other than the Applicable Laws of India), irrespective of where Data Principals are based. Data Principal specifically waives any rights which are granted to Data Principal under any laws (other than the Applicable Laws of India) and further acknowledges the adequacy and sufficiency of the Applicable Laws of India to protect, inter alia, the Data Principal's privacy rights.

19. Compliances With Applicable Laws

19.1 Notwithstanding anything stated hereinabove and for the avoidance of doubt, all obligations of Saatvik and Data Principal (if any), as stated herein, are and will be subject to compliance with all Applicable Laws (including in particular the DPDP Act, the IT Act, the IT Rules and the Consumer Protection (E-Commerce) Rules, 2020) as may be amended, modified, consolidated, substituted and re-enacted from time to time.

19.2 The Company shall not be responsible for complying with the laws of any jurisdictions (other than the Applicable Laws of India), irrespective of where the Data Principal is based, and any rights which are granted to the Data Principal under any foreign laws are hereby expressly and unconditionally waived by the Data Principal.

20. Documentation

Adequate relevant policies, procedures, work instructions, templates, formats, etc., need to be defined and framed covering the following:

20.1 An appropriate organizational structure, mechanism to ensure compliance of the Data Privacy program

20.2 All employees and third-party contractors must report suspected data breaches within 24 hours to the DPO. Where legally required, Saatvik will notify regulators and affected individuals within statutory timelines.

20.3 Data breach response plan

20.4 A data breach risk register, which should contain the risk assessment and treatment plan depending upon the severity and impact of a data breach

20.5 Develop a governance model (matrices, reports and dashboards) for tracking the data protection program performance

20.6 Defining an internal audit mechanism for maintaining the data privacy program

21. Reference

Sr. No.	Name	Document Id
a)	**Document**	
b)	**Templates**	

Disclaimer:

This document is solely for the information of Saatvik Green Energy Limited and its subsidiaries and should not be used, circulated, quoted, or otherwise referred to for any other purpose, nor included or referred to in whole or in part in any document without our prior written consent.

Confidentiality:

This document contains restricted information pertaining to Saatvik Green Energy Limited and its subsidiaries. The access level for the document is specified in the document. The addressee should honour this access rights by preventing intentional or accidental access outside the access scope.