

Privacy Policy

The Clearing Corporation of India Ltd. (CCIL) adheres to the stringent principles governing its operations as a financial market infrastructure regulated by the Reserve Bank of India (RBI). It has two wholly owned subsidiaries- Clearcorp Dealing Systems (India) Ltd. (Clearcorp), which facilitates the business of providing dealing systems/platforms and Legal Entity Identifier India Ltd. (LEIL) which acts as a Local Operating Unit (LOU) for issuing globally compatible Legal Entity Identifiers (LEIs) in India. CCIL, Clearcorp and LEIL are ISO/IEC 27001 institutions. **Any reference to “CCIL” hereinafter, in this Privacy Policy (Policy) shall be deemed to also include a reference to its wholly owned subsidiaries Clearcorp and LEIL as the case may be.** This Privacy Policy provides the practices and policies applicable to CCIL for handling of or dealing in Personal Information, including Sensitive Personal Data or Information (as defined below) that is lawfully collected by CCIL.

GENERAL DEFINITIONS

Reference to “**you**” or “**your**” in this Privacy Policy refers to any natural person (including the employees of CCIL) who provides to CCIL any information referred in **Schedule 1** of this document or any user(s) of CCIL’s website or business applications whether or not, you avail the Services offered by CCIL.

“Act” shall mean the Information Technology Act, 2000 and Rules thereunder as amended from time to time.

“Information” shall mean and include Personal Information and Sensitive Personal Data or Information as may be collected by CCIL.

“Personal Information (PI)” shall have the same meaning as under Rule 2 (i) of the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 as amended from time to time. For ease of reference Rule 2 (i) of the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 is re-produced under Schedule 1.

“Rules” shall mean the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 as amended from time to time.

“Registered User” shall mean such user whose registration is accepted by CCIL and who accesses CCIL’s web portal/business applications based on the password based authentication chosen.

“Sensitive Personal Data or Information (SPDI)” shall mean and include information under Rule 3 of the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 as amended from time to time. For ease of reference

Rule 3 of the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 is re-produced under Schedule 1.

“Services” for the purpose of this Privacy Policy shall mean

- a. the services of CCIL which has been sought by any person either by way of registration on CCIL’s website or any other mode/platform of CCIL or any other means (electronic or otherwise)
- b. any engagement/arrangement of CCIL with any person, wherein CCIL has sought services and for the limited purpose of this Policy shall include services from suppliers, consultants, vendors etc. as the case may be.

All words and expressions used and not defined in this document but defined in the Act or the Rules shall have the meanings respectively assigned to them in the Act or the Rules.

Notwithstanding anything contained herein, Employees of CCIL shall also be covered under this Policy and the contents of this Policy shall be applicable mutatis mutandis to Employees, unless the context requires otherwise.

CCIL is fully committed to respecting your privacy and shall ensure that your Information is safe. This privacy policy sets out the practices adopted in respect of Information, including the types of Information that is collected, the mode/method of collection of Information, usage of Information, sharing and retention of Information, etc. This Privacy Policy is published in compliance with the provisions of the Act and the Rules made thereunder that require publishing the privacy policy on CCIL’s website. **CCIL urges you to read this Privacy Policy carefully before you use or opt to access any services of CCIL or decide to part with any Personal Information including the information listed under Schedule 1.**

1. COLLECTION OF INFORMATION

- 1.1** You may use CCIL’s website to access information, learn about its products and services, read publications and check career opportunities etc. without providing any PI/SPDI.
- 1.2** CCIL may collect and process PI/ SPDI provided by you in the following forms:
 - (a) Should you opt to access such services of CCIL, which are available only to Registered Users, Information is required to be provided by you at registration such as your name, date of birth, address, email ID, gender and phone number. Providing additional information beyond what is required at the time of registration is entirely optional and can be altered or removed by you at any time. Registered Users are given access to the web portal/business applications based on the password based authentication which is chosen by them and securely stored in CCIL servers for the purpose of authentication of the Registered Users at the time of login;

- (b) Information that you provide directly to CCIL via email or electronic communication;
- (c) Information that you provide to CCIL over telephone. CCIL may make and keep a record of such information shared by you;
- (d) Information that you provide to CCIL in physical form whether sent through post or courier or handed over to a CCIL representative in person; and
- (e) PI/SPDI collected by CCIL from its employees, suppliers or onsite consultants for the purpose of employment, availing their services and recording their attendance etc.
- (f) PI/SPDI received by CCIL from any person seeking career opportunities or provided by its employees through background verification or security checks.
- (g) Information collected by CCIL in respect of Disaster recovery plan, crisis management, internal and external communications.
- (h) For any other purposes as CCIL may deem necessary.

CCIL only collects, uses and discloses PI/SPDI for purposes that are reasonable and legitimate. Such PI/SPDI shall be processed in a manner compatible with the purposes for which it has been collected; unless the individual providing such PI/SPDI has consented to it being processed for a different purpose or the use for a different purpose is permitted by applicable law. There may be circumstances, when an individual may have volunteered personal information and given explicit/fully informed consent to its processing (for example by submission of a CV).

You will at all times have the option of not providing CCIL with PI/SPDI that CCIL seeks to collect. Even after you have provided CCIL with any PI/SPDI, you will have the option to withdraw the consent given earlier. In such cases, CCIL will have the right to not provide or discontinue the provision of any service that is linked with such PI/SPDI. In any case, CCIL will not be liable and or responsible for the denial of certain Services to you for lack of you providing the necessary PI/SPDI.

2. USE OF INFORMATION COLLECTED

- 2.1** Any Information, if collected will be used in connection with the relevant purpose as per the contract and as under Section 1.2. The provider of Information availing any Services from CCIL shall be deemed to have consented to CCIL for the use of such Information as under this policy.
- 2.2** Employees, suppliers or consultants of CCIL shall be duly advised about the purpose for which any Information is being collected at the time of such collection.

3. SHARING/ DISCLOSURE OF INFORMATION

- 3.1** CCIL may share/disclose your Information, where such Information is required to be shared/disclosed arising out of any contractual obligation or for the purposes of providing Services
- 3.2** To the extent necessary to provide you the requested Services or to the extent required under applicable law, we may provide your PI/SPDI to the following Third Parties without notice to you:
- (a) Consultants (including auditors, authorized vendors) on a 'need to know' basis under a Non-Disclosure Agreement;
 - (b) Governmental authorities, in such manner as permitted or required by applicable law; and
- 3.3** Legal proceedings: In the event, CCIL is required to respond to subpoenas, court orders or other legal process, your PI/SPDI may be disclosed pursuant to such subpoena, court order or legal process, which may be without notice to you.

4. SECURITY OF INFORMATION

- 4.1** CCIL strives to ensure the security, integrity and privacy of your PI/SPDI and to protect your Information against unauthorized access, alteration, disclosure or destruction. Stringent security measures (physical, electronic and managerial) are in place to protect against the loss, misuse, and alteration of the PI/SPDI under our control. CCIL's servers are accessible only to authorized personnel and your Information is shared with employees and authorized personnel strictly on a 'need to know' basis.
- 4.2** As a technology driven financial market infrastructure CCIL uses and has a comprehensive documented information security program and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the Information being protected. CCIL periodically assesses, audits and updates its information security protocols and policies to achieve the highest standards on a continuous and ongoing basis.
- 4.3** The PI/SPDI provided to CCIL shall be accurate, not misleading, updated and complete. CCIL shall be updated as and when such PI/SPDI provided earlier becomes incorrect or out of date, by providing new details. You may review the Information you have provided to CCIL at any time. On your request, CCIL will ensure that any PI/SPDI notified to be inaccurate or deficient, shall be corrected or amended. However, CCIL shall not be responsible for the authenticity of the PI/ SPDI.
- 4.4** Notwithstanding anything contained in this Privacy Policy or elsewhere, CCIL shall not be held responsible for any loss, damage or misuse of your PI/SPDI, if such loss, damage or misuse is attributable to a Force Majeure Event.

5. RETENTION AND REVOCATION OF INFORMATION

- 5.1** Your PI/SPDI will be retained with CCIL as long as you avail the Services of CCIL or for such period as may be necessary under applicable law. Once CCIL no longer requires PI/SPDI, it is destroyed appropriately and securely.
- 5.2** In the event, you wish to no longer avail the Services of CCIL or intend to request that CCIL no longer retain your PI/SPDI or where you intend to modify the current PI/ SPDI, you may contact CCIL as provided herein below.

6. NOTIFICATION OF CHANGES

- 6.1** This Policy shall be reviewed annually. The Policy may be amended as may be considered necessary upon such review or upon any change in applicable law from time to time. Modifications, if any, in the Policy shall be approved by the Board of Directors in its ensuing meeting. The Last Updated Date of this Policy, stated below (6.3), indicates the last time this policy was revised or materially changed. Checking the effective date below allows you to determine whether there have been changes since the last time you viewed the Policy.
- 6.2** In the event, if you object to any of the changes, and you no longer wish to use the Services or intend to revoke your consent to retain your PI/SPDI with CCIL, you may contact CCIL as provided hereunder.
- 6.3** **Last Updated Date: October, 2024**

7. INQUIRIES

CCIL respects and is sensitive to the rights as granted in the data protection laws. Should you have questions about the Privacy Policy or CCIL's information collection, use and disclosure practices, you may contact the Grievance Officer as per the details given herein below. CCIL will use reasonable efforts to respond promptly to requests, questions or concerns you may have regarding the use of your PI/SPDI.

8. GRIEVANCE OFFICER

In accordance with the Information Technology Act, 2000 and the rules made thereunder, the name and contact details of the Grievance Officer are provided below. You may contact the Grievance Officer to address any discrepancies and grievances you may have with respect to your Information with CCIL.

Name – Mr. Dinesh Phogat
[Chief Information Security Officer- Risk Management]

Contact Number: [+91 22 61546445]
Email ID: [dphogat@ccilindia.co.in]

Schedule 1

Rule 2 (i)

“Personal information” means any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.

Rule 3

Sensitive personal data or information of a person means such personal information which consists of information relating to: -

- (i) password;
- (ii) financial information such as Bank account or credit card or debit card or other payment instrument details;
- (iii) physical, physiological and mental health condition;
- (iv) sexual orientation;
- (v) medical records and history;
- (vi) Biometric information;
- (vii) any detail relating to the above clauses as provided to body corporate for providing service; and
- (viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise:

Provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.