

Terms of Use - Requester

Updated on 2nd June 2025

These terms govern Requesting entity's participation as a Requester in DigiLocker, a digital document wallet service provided by the National e-Governance Division (NeGD) under the Ministry of Electronics and Information Technology (MeitY), Government of India. By integrating with or issuing documents to DigiLocker, Requester agrees to comply with all applicable terms, policies, and guidelines set forth by NeGD.

All components of the DigiLocker platform, including but not limited to data, text, document templates, designs, pages, graphics, user interfaces, visual elements, images, artwork, photographs, trademarks, logos, audio and video content, HTML code, source code, and software (collectively referred to as “Content”) that are accessible through or embedded in the DigiLocker platform, are the intellectual property of the National e-Governance Division, MeitY. Requesters may utilize the platform solely for the purpose of digitally issuing documents to end-users in accordance with DigiLocker policies, without acquiring any ownership rights over the platform or its Content.

1. SCOPE

These Terms and Conditions govern the onboarding of the Requester Organization onto the DigiLocker platform. Upon successful onboarding, the Requester shall be authorized to access documents disseminated directly from end-users through the DigiLocker platform.

DigiLocker, shall act solely as a secure transmission platform for such documents. Responsibility for the content and validity of issued documents rests solely with the Issuer.

2. REQUESTER ONBOARDING AND ELIGIBILITY

Requester Organizations must designate a senior authorized representative to initiate and complete onboarding onto the DigiLocker platform. Registration must be conducted using the official email domain of the organization, and all submitted information is subject to verification by NeGD. Misrepresentation may result in suspension or denial of access.

3. PERMITTED USE OF DIGILOCKER APIS

Requester Organizations are granted access to DigiLocker APIs solely for the purpose of retrieving documents disseminated through DigiLocker. All integrations must preserve DigiLocker branding and may not be rebranded or modified without prior written consent. Use of the API for unauthorized purposes is strictly prohibited.

4. ROLES AND RESPONSIBILITIES

- a) NeGD shall provide the DigiLocker platform, technical documentation, and necessary API access to facilitate the Requester's secure access to user documents.
- b) NeGD shall ensure that access to user data or documents is strictly governed by user consent in compliance with applicable laws and shall monitor the platform to prevent misuse.
- c) The Requester shall integrate its systems with DigiLocker's Requester APIs and shall obtain explicit and informed user consent prior to accessing any document.
- d) The Requester must clearly inform users of the purpose of data access and must not cache, duplicate, or store documents beyond the permitted duration.
- e) The Requester shall implement adequate technical and organizational safeguards to ensure the protection of user data and shall promptly notify NeGD of any security incidents within twenty-four (24) hours of discovery. Compliance with applicable Indian Laws and other relevant regulations is mandatory.
- f) The Requester agrees to comply with the DigiLocker Terms of Use and relevant API Specifications, as updated from time to time as fixed by NeGD/DigiLocker.

5. ACCESS RESTRICTIONS AND MISUSE

Requesters must not engage in any activity that compromises the integrity, availability, or confidentiality of the DigiLocker system. Unauthorized access, reverse engineering, data scraping, or misuse of API endpoints will result in immediate suspension and potential legal action.

6. CONSENT AND LEGAL LIABILITY

- a) The Requester acknowledges and agrees that DigiLocker shall not be liable for the contents, misuse, or misrepresentation of any documents once delivered through its system.
- b) Documents fetched or issued via DigiLocker shall be accessible solely through explicit user consent, with consent-based access enabled via DigiLocker. The Requester must ensure that no data or document is stored, cached, or reproduced outside the transaction except where explicitly required by applicable laws or regulations.
- c) These Terms further affirms the Parties' intent to align with the principles of consent-based data sharing in compliance with the Data Protection Laws as currently prevalent in India, Public Key Infrastructure (PKI) for digital signing and verification, and standardization of electronic document formats. All integrations and data exchanges shall follow the applicable Indian laws.
- d) The Requester confirms that DigiLocker will operate only upon such user consent and shall not be held accountable for any legal claims arising from the issuance or delivery of documents.

- e) The Requester shall at all times indemnify and keep DigiLocker indemnified of any legal claims arising from the issuance or delivery of documents in furtherance to utilizing the DigiLocker services.

7. GENERAL PROVISIONS

- a) The Requester acknowledges and understands that it must be able to fulfil their responsibilities under these terms in accordance with the provisions of the law and regulations that govern their activities. Nothing in these Terms intends to negate or otherwise render ineffective any such provisions or operating procedures. The Requester assume full responsibility for their performance under these Terms.
- b) If at any time requester is unable to perform its duties or responsibilities under these terms consistent with such statutory and regulatory mandates, NeGD shall immediately provide written notice to establish a date for resolution of the matter.

8. JURISDICTION

These Terms shall be governed by and construed in accordance with the laws of India and the Courts at New Delhi shall have exclusive jurisdiction over all legal disputes under these Terms.

9. COMMERCIALS/ PAYMENT TERMS:

Currently, there are no platform charges applicable. However, should any such charges be introduced in the future, the Requester Organization will be duly informed in advance prior to the implementation of such charges. Such charges would always be prospective in nature.

10. GRIEVANCE REDRESSAL MECHANISM

The Requester agrees that grievances will be addressed and resolved, in compliance with applicable legal and regulatory requirements. In the event you have any questions or concerns about these Terms, or if you need support or wish to file a grievance, please contact us at: partners@digitallocker.gov.in

Address: National e-Governance Division (NeGD), Ministry of Electronics and Information Technology (MeitY), Government of India, New Delhi, India.

11. RESPECT FOR DATA PRINCIPAL RIGHTS

The Requester affirms its commitment to support individuals in exercising their rights under applicable data protection laws, including access, correction, and grievance redressal, through appropriate and timely mechanisms.

12. PRIVACY NOTICE AND TRANSPARENCY

The Requester shall provide a clear, comprehensive, and easily accessible privacy notice to all Data Principals prior to the collection or processing of any personal data under these Terms. This notice shall set out, at a minimum, the categories of personal data being collected, the purposes for which such data is being processed, the lawful basis for such processing, the entities with whom the data may be shared, the duration for which the data shall be retained, and the rights available to the Data Principal under the applicable law. The privacy notice shall be written in simple and unambiguous language and made available in a manner that is easily accessible to all users.

13. PERSONAL DATA BREACH NOTIFICATION

In the event of any actual or suspected personal data breach involving personal data processed pursuant to these Terms, the Requester shall promptly notify DigiLocker in writing within twenty-four (24) hours of becoming aware of the breach. Furthermore, the Requester shall comply with all legal obligations to report such a breach to enable NeGD to take necessary action accordingly.

14. COMPLIANCE AND OVERSIGHT

The Requester agrees to implement appropriate technical, organizational, and administrative safeguards to ensure the confidentiality, integrity, and security of personal data processed in connection with these Terms. Requester further agrees to abide by all applicable laws and regulations governing the handling of personal data. DigiLocker reserves the right to conduct, or cause to be conducted, periodic audits of the Requester to assess compliance with the terms of these Terms and applicable data protection obligations.

15. AUDIT REQUIREMENTS

The Requester shall conduct an annual compliance audit of its DigiLocker integration and practices, including data protection mechanisms and access control, through an CERT-IN empaneled auditor. The audit report may be verified by NeGD and Non-compliance may lead to suspension of API access until rectification.

16. TERMINATION AND SUSPENSION

Termination: NeGD may terminate this engagement, in whole or in part, with immediate effect upon the occurrence of a material breach of these Terms by the Requester. A material breach shall include, but not be limited to:

1. **Failure to Perform Obligations:** Any lapse, negligence, or failure on the part of the Requester to fulfill their responsibilities or obligations under these Terms.

2. Breach of Representations: Any misrepresentation, incorrect statement, or breach of undertakings provided by the Requester.
3. Receipt of direction from competent/ regulatory authority, which, in the sole discretion of NeGD, indicates non-compliance or potential risk.
4. Legal or Regulatory Non-Compliance: Any act or omission by the Requester which may result in a breach of applicable laws, rules, regulations, or guidelines.

In the event of any of the above, NeGD shall issue a Rectification Notice, allowing the Requester a period of 7 (seven) days from the date of such notice to rectify the identified breach or lapse to the satisfaction of NeGD.

Failure to adequately rectify the breach within the stipulated period shall result in the complete suspension and/or termination of the engagement without any further notice or obligation on the part of NeGD.

NeGD reserves the right to suspend or block API access without prior notice in case of non-compliance, security concerns, or directions from competent authorities.

Termination or suspension under this clause shall be without prejudice to any other rights or remedies available to NeGD under applicable law.

Suspension: As mentioned earlier, NeGD reserves the right to temporarily suspend or permanently revoke access to the DigiLocker platform in case of serious non-compliance by the Requester, such as repeated failure in audit, data breaches, or legal violations.

17. USAGE BY SUBSIDIARIES / AFFILIATED ENTITIES

The Requester may extend DigiLocker integration for use by affiliated departments or agencies only upon prior written approval by NeGD. The Requester shall remain liable for all activities and usage undertaken through its issued APIs or credentials.

18. DATA PROTECTION AND CONFIDENTIALITY

Requester Organizations must ensure the confidentiality and security of any personal or sensitive data accessed or transmitted through DigiLocker. All data processing must comply with applicable data protection laws as applicable in India. Data must not be stored or transmitted outside India without authorization.

19. AMENDMENT OF TERMS

DigiLocker, may update these Terms periodically to reflect changes in services, legal requirements, or policies. NeGD reserves the right to revise the Terms at its discretion, with updates notified via the DigiLocker website. Requester's are responsible for reviewing the Terms regularly. Continued use of DigiLocker services implies acceptance of the updated Terms.

